(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002044071 A**

(43) Date of publication of application: **08.02.02**

(51) Int. Cl **H04L 9/16**
H04L 9/08
H04N 5/44
H04N 5/765
H04N 5/91
H04N 7/16
H04N 7/167

(21) Application number: **2000370282**

(22) Date of filing: **05.12.00**

(30) Priority: **16.05.00 JP 2000148600**

(71) Applicant: **HITACHI LTD**

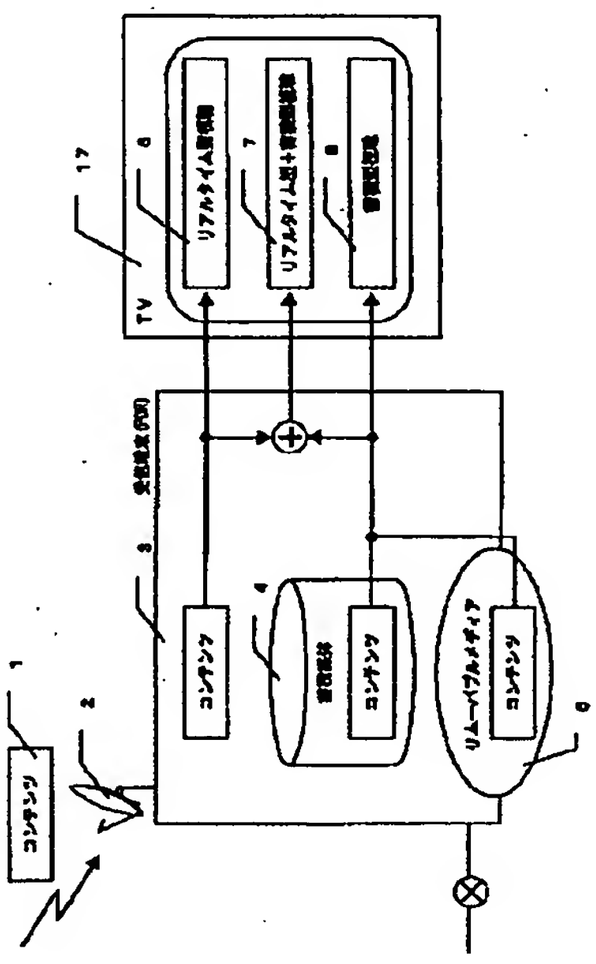
(72) Inventor: **HARADA HIROMI**
KONISHI KAORU
YAMAZAKI IORI

(54) **RECEIVING METHOD**

(57) Abstract:

PROBLEM TO BE SOLVED: To protect a copyright by enciphering various contents with another key and making portable a restricted receiving (CA) module.

SOLUTION: For performing enciphering for each of contents, the contents are enciphered on the transmitting side, meta-data are transmitted simultaneously with the enciphered contents, and the enciphered contents and the meta-data are stored on the side of a receiving terminal, which receives contents information. When viewing the stored enciphered contents, the meta-data are enciphered while using a disposable key prepared inside the receiving terminal and the enciphered contents and the meta-data are separated. In the case of transfer to a third person, the personal information of the transfer destination first received without including owner information is stored. Since enciphering is enabled for each of contents by a unique key and a second CA module capable of specifying an individual is combined, service providing to an individual and transfer to the third person are enabled.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－44071
(P2002－44071A)
(43)公開日　平成14年２月８日(2002.2.8)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
H04L	9/16		H04N	5/44	Z　5C025
	9/08			7/16	C　5C053
H04N	5/44		H04L	9/00	643　5C064
	5/765				601A　5J104
	5/91				601E

審査請求　未請求　請求項の数10　ＯＬ　(全 30 頁)　最終頁に続く

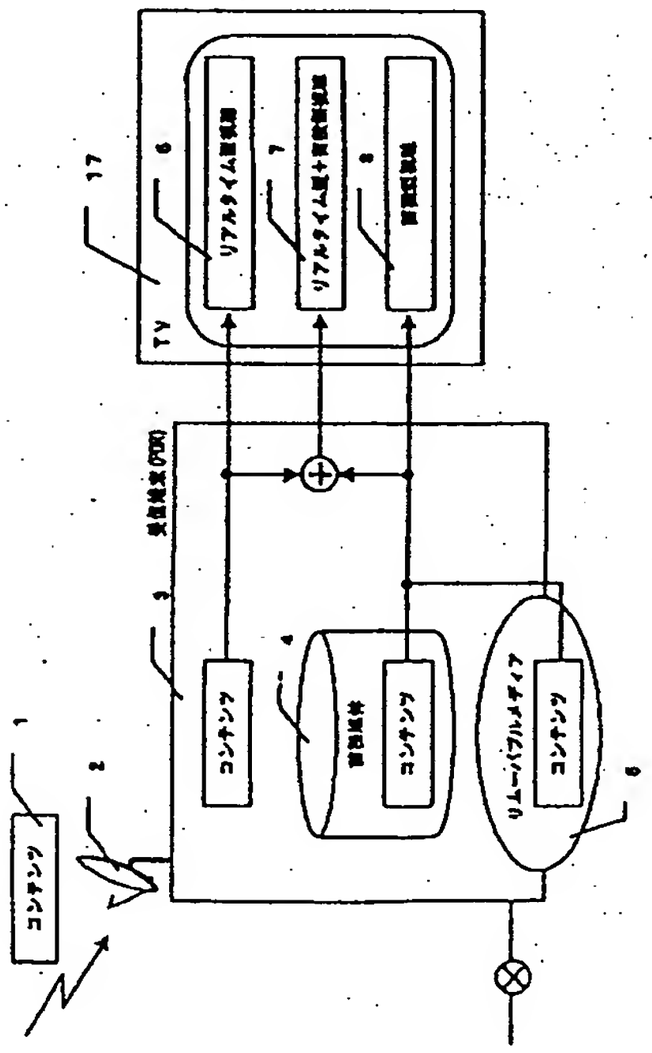
(21)出願番号　特願2000－370282(P2000－370282)
(22)出願日　平成12年12月５日(2000.12.5)
(31)優先権主張番号　特願2000－148600(P2000－148600)
(32)優先日　平成12年５月16日(2000.5.16)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　原田　宏美
東京都千代田区神田駿河台四丁目６番地
株式会社日立製作所放送・通信システム推進事業部内
(72)発明者　小西　薫
東京都千代田区神田駿河台四丁目６番地
株式会社日立製作所放送・通信システム推進事業部内
(74)代理人　100107010
弁理士　橘爪　健

最終頁に続く

(54)【発明の名称】　受信方法

(57)【要約】
【課題】　様々なコンテンツに別の鍵で暗号をかけ、限定受信（ＣＡ）モジュールを可搬可能とし、著作権を保護する。
【解決手段】　コンテンツ毎の暗号化を行うために、送信側でコンテンツを暗号化し、暗号化されたコンテンツと同時にメタデータを送信し、コンテンツ情報を受信した受信端末側で暗号化コンテンツとメタデータ蓄積を行う。蓄積された暗号化コンテンツを視聴する際に、メタデータに、受信端末内で作成した使い捨て鍵を用いて暗号化し、暗号化コンテンツとメタデータの分離化を行う。また、第３者への譲渡に対しては、所有者情報を入れずに最初に受け取った譲渡先の個人情報が格納される。コンテンツ毎にユニークな鍵で暗号化可能とし、個人を特定できる第２のＣＡモジュールを組合わせることで、個人に対するサービス提供、第３者への譲渡を可能とする。



【特許請求の範囲】
【請求項１】選択されたコンテンツに対応する暗号化メタデータを第１の使い捨て鍵（Kt）で復号するステップと、
メタデータに基づきコンテンツの視聴可否を判断し、課金情報を含む契約情報を作成し、メタデータに含めるステップと、
作成されたメタデータを第１及び第２の分離メタデータに分離するステップと、
第２の使い捨て鍵(Kt')を生成するステップと、
第２の分離メタデータを第２の使い捨て鍵(Kt')で暗号化した第２の分離メタデータを生成し、記録媒体及びリムーバブルメディアに蓄積するステップと、
第１の分離メタデータに第２の使い捨て鍵(Kt')を含め、入力された第３の個人鍵(Km2)で暗号化し、第２のモジュールに記録するステップと、
記録媒体に蓄積された暗号化コンテンツをリムーバブルメディアに蓄積するステップとを含む受信方法。
【請求項２】メタデータは、検索情報及び／又は課金情報を含む契約情報を含み、契約情報に従い、コンテンツ毎に課金処理を行うことを特徴とする請求項１に記載の受信方法。
【請求項３】第１のモジュールは受信機内に備えられ、第２のモジュールは可搬形で受信機に脱着可能であることを特徴とする請求項１又は２に記載の受信方法。
【請求項４】第１の受信機により暗号化された第１の分離メタデータ及び第３の個人鍵(Km2)が記録された第２のモジュール、及び、コンテンツ鍵(Kk)を含む暗号化された第２の分離メタデータ及び暗号化コンテンツが蓄積されたリムーバブルメディアを第２の受信機に装着するステップと、
第２のモジュールに記録された暗号化された第1の分離メタデータを第３の個人鍵(Km2)で復号化して第1の分離メタデータを生成し、
第１の分離メタデータに含まれた第２の使い捨て鍵(Kt')を用いて復号化して第２の分離メタデータを生成するステップと、
第１及び第２の分離メタデータに基づいてコンテンツの視聴の可否を判断するステップと、
復号化された第２の分離メタデータに含まれるコンテンツ鍵(Kk)を用いてリムーバブルメディアに記録された暗号化コンテンツを復号化してコンテンツを生成するステップを含む請求項１乃至３のいずれかに記載の受信方法。
【請求項５】選択されたコンテンツに対応する暗号化メタデータを第１の使い捨て鍵（Kt）で復号するステップと、
メタデータに基づきコンテンツの視聴可否を判断し、課金情報を含む契約情報を作成し、メタデータに含めるステップと、
作成されたメタデータを第１及び第２の分離メタデータに分離するステップと、
ギフト鍵を生成し、リムーバブルメディアに蓄積するステップと、
第２の分離メタデータをギフト鍵で暗号化し、リムーバブルメディアに蓄積するステップと、
第１の分離メタデータに第２の使い捨て鍵(Kt')を含め、入力された第２の個人鍵(Km2)で暗号化し、第２モジュールに記録するステップと、
記録媒体に蓄積された暗号化コンテンツをリムーバブルメディアに蓄積するステップとを含む請求項１乃至３のいずれかに記載の受信方法。
【請求項６】リムーバブルメディアに記録された暗号化された第２の分離データを復号化し、第２の分離メタデータを生成するステップと、
第２のモジュールに記録された暗号化された第１の分離メタデータを復号化し、第１の分離メタデータを生成するステップと、
第１及び第２の分離メタデータに基づき、コンテンツの視聴可否を判断するステップと、
リムーバブルメディアに記録された暗号化コンテンツを、コンテンツ鍵で復号化してコンテンツを生成するステップとを含む請求項１乃至５のいずれかに記載の受信方法。
【請求項７】コンテンツを、メタデータと同一の鍵で暗号化して、その鍵をコンテンツ配信時とは別の時間枠、別の配信場所又は別の配信手段で配信することを特徴とする請求項１乃至６のいずれかに記載の受信方法。
【請求項８】暗号化コンテンツをリムーバブルメディアに蓄積する際、記録媒体内の暗号化コンテンツ及び暗号化メタデータを複写して使用することを特徴とする請求項１乃至７のいずれかに記載の受信方法。
【請求項９】受信機内の第１のモジュールに記憶された第２の個人鍵(Kml)を用いて、受信されたスクランブル鍵(Ks)を復号化し、スクランブル鍵(Ks)を用いて復号化することにより、暗号化コンテンツ及び暗号化メタデータを含むイベントを生成するステップと、
受信機内に記憶された第１の個人鍵(Kmc)を用いて、受信された第１の暗号化ワーク鍵(Kwc')を復号化して第１のワーク鍵(Kwc)を生成するステップと、
復号化された第１のワーク鍵(Kwc)を用いて、共通情報として受信された第１の暗号化コンテンツ鍵（Kk'）を復号化して第１のコンテンツ鍵（Kk）を生成するステップと、
暗号化メタデータを第１のワーク鍵(Kwc)で復号化してメタデータを生成するステップとをさらに含む請求項１乃至８のいずれかに記載の受信方法。
【請求項１０】受信機内の第１のモジュールに記憶された第２の個人鍵(Kml)を用いて、受信されたスクランブル鍵(Ks)を復号化し、スクランブル鍵(Ks)を用いて暗号

化コンテンツ及び暗号化メタデータを含むイベントを生成するステップと、
受信機内に記憶された第１の個人鍵(Kmc)を用いて、受信された第１の暗号化ワーク鍵(Kwc')を復号化し第１のワーク鍵(Kwc)を生成するステップと、
復号化された第１のワーク鍵(Kwc)を用いて、暗号化メタデータを復号化し、そこに含まれた第１のコンテンツ鍵（Kk）を求めるステップとをさらに含む請求項１乃至８のいずれかに記載の受信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、受信方法に係り、特に、デジタル放送により暗号化コンテンツを視聴するための受信方法に関する。
【０００２】
【従来の技術】従来のデジタル放送では、サービスチャンネル毎に視聴可／不可の契約を行う契約形態、もしくは同一チャンネル内での時間毎の番組契約を行う契約形態が存在していた。また、既存のデジタル放送等では、各々のコンテンツ単位でのコンテンツの購入を行わせるために、ユーザーがサービス選択後に欲しいコンテンツを選択、契約又は決定し、その契約又は決定と同時にセンタ側との通信を行うようにしている。ユーザーとセンタ側とのリアルタイム通信によって各コンテンツの購入を確認し、確認後契約者に購入許可データを送信することで、ユーザーはコンテンツを購入可能となる。このような双方向リアルタイム購入方式でコンテンツ単位での販売が行われることとなる。
【０００３】暗号化に関しては、今後始まるデジタル放送において、ネットワーク内で使用可能な暗号鍵は数が固定されているため、伝送路で暗号化する／しないの判断がなされる。また、現在の伝送方式では、センタ側で暗号化されたコンテンツは、受信端末内で受信後直に暗号解除を行った後に蓄積装置等に記録される。このように伝送時におけるコンテンツの暗号化は、現在１次暗号のみで行なわれている。
【０００４】
【発明が解決しようとする課題】しかしながら、従来のデジタル放送では、契約時間内での全てのサービス情報を取得することができるが、ユーザーが選択したサービス情報のみの視聴もしくはコンテンツのみの入手は困難である。
【０００５】また、従来のＣＳ／ＢＳなどのデジタル放送でのサービスにおいては、契約形態がチャンネル視聴可／不可、または同一チャンネル内の番組視聴可／不可の契約提供がメインとなっている。これはデジタル放送内における暗号化に用いる鍵の数に制限があるためである。ただし複数の鍵を使用すると鍵の管理が複雑となるだけでなく、複数鍵でのコンテンツの暗号化を行うことで暗号を解くために必要な情報の常時送信となり、現在の伝送量よりさらに多くの情報を伝送しなくてはならない。これは少ない伝送領域においては、困難に近く現実的ではない。また、日々増加するコンテンツ毎に鍵をかけることは、鍵の数が無限大に近くなることであり、これも管理が非常に難しい。さらに、リアルタイム復号に必要な情報を常に伝送しているため、受信端末は、受信時に復号化に必要ＩＣカード等のモジュール（ＣＡ（Conditional Access，限定受信）モジュール）を常時取り付けさせる必要がある。これらのことより、同じチャンネル内の同じ番組の同じ時間において複数の鍵を用いてコンテンツの暗号化を行うことは、困難に近い。
【０００６】また、従来の受信端末では、暗号解除後に再度受信端末内で暗号化を行うことが出来ない。これより受信端末等に存在する蓄積コンテンツを一度復号化した後に、再度暗号化させて蓄積をさせることは不可能であり、また伝送路の暗号化のまま蓄積すると蓄積時における暗号化の鍵扱い等がむずかしくなり、暗号化させて蓄積させるには信頼性等様々な課題が多い。また、デジタル放送を受信する場合において視聴可／不可等の契約を扱う情報が受信端末毎でしか行えないため、受信端末を利用するユーザーが複数の場合、センタ側で複数ユーザー毎の契約形態を認識できない等の課題がある。
【０００７】さらに、例えばコンテンツの第３者に対する譲渡場合等において要求される、著作権保護の方式として電子透かし等のパスワード埋め込みの形式は存在するが、全てのデータ形式に対して有効ではなく、コンテンツのみの保護でしかない。システムとしてコンテンツ並びにコンテンツ関連情報（メタデータ）の両方を保護する方式は現状存在しない。
【０００８】本発明は以上のような課題を解決することを目的とする。例えば、本発明は、受信端末内で生成した使い捨て鍵を用いてメタデータの作成並びに分割化を行うことで、コンテンツ毎に暗号化可能とする。また、本発明によると、個人を特定できる第２のＣＡモジュールを合わせることで個人特定のサービスを行うようにすることを目的とする。
【０００９】さらに、本発明は、メタデータ内にコンテンツの所有者情報を入れずにおくことで、コンテンツの譲渡をされた方の受け取り時に初めてコンテンツ所有者が特定できるようにし、ＣＡモジュールへの所有者情報記入が行なわれることにより、第３者への譲渡目的としたコンテンツサービスを実現することを目的とする。
【００１０】
【課題を解決するための手段】本発明は、暗号化コンテンツとそのコンテンツの視聴のために必要なコンテンツ関連情報であるメタデータとによりコンテンツを定義し、また、個人を特定した第２のＣＡモジュールを使用する。これにより、個々に対するサービスの提供を可能とし、また第３者に対する譲渡を目的としたコンテンツの受け渡しにおけるセキュリティ保護も施し、第３者に

譲渡を行うサービスの提供を可能とする。

【００１１】ここで、メタデータとは、基本的にコンテンツ以外の情報の総称であり、例えば、コンテンツ制御情報、コンテンツ内容情報、コンテンツ関連情報として定義することができる。概念的には受信端末側でコンテンツを制御するための情報で、例えばコンテンツの蓄積予約を行うための情報（EPG（Electronic Program Guide、電子番組ガイド）に表示するためのコンテンツの名前、ジャンル、配信場所、配信予定日時）、利用制限情報（視聴が可能となるための条件、２０歳以上、男性、○○放送局との契約者）、暗号の鍵等の情報が含まれる。

【００１２】本発明においては、コンテンツ毎の暗号化を行なうために、暗号化コンテンツとそのコンテンツに対する視聴契約形態等の情報を含むコンテンツ関連情報（メタデータ）の分離化を行なう。最初に送信側でコンテンツの暗号化を行ない、暗号化されたコンテンツと同時にメタデータを送信する。この情報を受信した受信側の受信端末では暗号化コンテンツの蓄積、メタデータの伝送路における伝送暗号の復号化および受信端末内で生成される使い捨て鍵による暗号化等の加工を必要に応じて行なった後、送信データの全ての蓄積を行なう。蓄積された暗号化コンテンツを視聴する際は、使い捨て鍵により暗号化されたメタデータを復号化し、有効期限、視聴回数制限、コピー制限、暗号化されたコンテンツを復号するための情報などを埋め込み、再び受信端末内で生成した使い捨て鍵を用いて、メタデータを元にメタデータ１、２の作成並びに分割化を行なう。暗号化コンテンツとメタデータ２をセットとして受信端末の記録媒体等に蓄積し、また残りのメタデータ１をＣＡモジュール等のユーザー個人特定蓄積媒体に書込む。

【００１３】このように、メタデータ１、２と暗号化コンテンツを合わせることで初めて視聴可能となるシステムとする。また、暗号化コンテンツと共に蓄積されるメタデータは受信端末内で生成される使い捨て鍵で受信端末内で暗号化を行なう。ＣＡモジュールに書込むメタデータ１はユーザー個人の鍵でＣＡモジュール内で暗号化を行なってもいいし、受信端末内でのコンテンツ管理機能で暗号化を行うことも可能である。また、暗号化を行わずにＣＡモジュール内に格納も可能である。受信端末側では、使い捨て鍵を生成しコンテンツ関連情報（メタデータ）に再度暗号化を行なうことで、コンテンツ毎に異なった暗号化を行なうことを可能とする。

【００１４】ユーザーが契約コンテンツを視聴する際には、検索／課金情報等、受信端末側でこれらの情報を生成し、受信端末内でメタデータ１、２などに基づき再生を行なう。よって受信端末内で複数の鍵を生成し、コンテンツ毎に暗号用の鍵として使用が可能となる。また、暗号化されたコンテンツをセンタ側より送信することで、受信端末内で大容量のコンテンツを暗号化する必要はなく、メタデータ、受信端末内で生成されるメタデータ１、２についてのみ使い捨て鍵や個人鍵で暗号化する。このメタデータの情報の解読で復号に必要な情報を入手可能となる。さらにコンテンツ毎に鍵が異なるが、この異なった鍵の全てがＣＡモジュール等に書込まれる。この書込まれた鍵の情報を使用して暗号化コンテンツの再生等を行なうが、再生時のみＣＡモジュール等を必要とするため、常時受信端末に設置する必要はなく、家庭でのコンテンツ購入だけでなく外部などの家庭外への持ち出しでのコンテンツの視聴契約が可能となる。これよりＣＡモジュール等の可搬による受信端末外部での契約も可能となる。よってＣＡモジュール等のユーザー個人特定蓄積媒体は持ち運びが可能となる。

【００１５】また、受信端末で蓄積した暗号化コンテンツは、ユーザーの視聴時に暗号化されたコンテンツを複写し、同様に暗号化されたメタデータ１、２も複写し、複写したメタデータ１、２を復号化したのち、復号化したメタデータ１、２を使用することにより、複写されたコンテンツを復号化して再生する。これより暗号化されたコンテンツデータは常時蓄積された状態となり、いつでも別のＣＡモジュールで同様のサービスを享受することが可能である。

【００１６】また、第３者に譲渡の目的でコンテンツを購入する際に、暗号化コンテンツと暗号化されたコンテンツに関する情報（メタデータ）と第３者に対する譲渡を目的にしていることを示すギフト情報で構成されたデータの組み合わせを行うことで譲渡目的としたサービスを行うことが可能となる。

【００１７】

【発明の実施の形態】以下の見出しに従い説明する。

１．システム
２．データ構成
３．暗号化・復号化
４．受信端末
５．コンテンツ蓄積・視聴
６．拡張サービス
７．まとめ

【００１８】１．システム

（サービス概要）図１に、蓄積型テレビ放送サービスの受信側の概要図を示す。この受信側は、アンテナ２、受信端末３、テレビ１７を備える。

【００１９】本サービスの概要として、蓄積型テレビ放送について説明する。従来のテレビ放送は、放送サイド（放送局）から送られてくるコンテンツ１（番組）をアンテナ２（ケーブルでの伝送の場合もある）、受信端末３で受信し、テレビ１７などのモニタ装置にて送られてきているその瞬間から視聴を行なう（ここでは、「リアルタイム型視聴６」と呼ぶ。）。蓄積型テレビ放送とは、従来のテレビ放送と同様のリアルタイム型視聴６に加え、従来のビデオデッキなどと同様に一度送られてき

たコンテンツを蓄積媒体４（本発明ではこれを、例えば、HDDとして説明する）に蓄積後視聴する「蓄積型視聴８」、蓄積されたコンテンツと送られてきているリアルタイムのコンテンツを合わせて視聴する「リアルタイム型＋蓄積型視聴７」などのサービスを可能とするテレビ放送である。なお、蓄積型視聴８では、ＤＶＤなどの可搬性に富んだリムーバブルメディア５を蓄積媒体として使用することもある。本発明では、上記のような蓄積型テレビ放送におけるサービス、特にコンテンツの暗号化、鍵の配信方式、契約方式などについて述べる。

【００２０】（システム概要）蓄積型テレビ放送サービスを行なうシステムとしては、衛星放送、地上波放送など電波によるインフラのほかに、ケーブルテレビ、インターネットなどの通信線を利用したインフラでのサービスが可能である。本発明では、一例として、デジタル衛星放送、特にBSデジタル放送をインフラとした場合について述べる。

【００２１】図２に、蓄積型テレビ放送サービスシステムの全体図を示す。まず蓄積型テレビ放送サービスが行なわれるシステムの全体を、この図を用いて説明する。

【００２２】蓄積型テレビ放送サービスシステムは、コンテンツを制作、配信する放送サイドであるセンタ側９と、受信側である受信端末３（PDR：personal digital recorder以後受信端末を略してPDRと呼ぶ場合もある。）を備える。センタ側９では上記の通りコンテンツ及び関連した情報の制作、配信の他に著作権、視聴制御、課金などを考慮した暗号化、鍵管理、ユーザーリクエスト受け付けなども行なわれ、そのコンテンツ及び関連した情報を配信可能なデータへ組み立て、および、衛星１０を介し受信端末３側に配信する。受信側である受信端末３は、衛星１０を介したコンテンツ及び関連した情報をアンテナ２により受信し、TV１７等のモニタ装置に直接出力、または蓄積媒体４内に蓄積後出力することで、ユーザーの視聴を可能とする。この受信端末３がTV１７等のモニタ装置に内蔵されることもあるが、ここでは別装置として説明する。

【００２３】蓄積型テレビ放送サービス用の受信端末３は、コンテンツ及び関連した情報を蓄積するための蓄積媒体４を有している他に、暗号／復号化モジュール２００、ＣＡモジュール１　１００、モジュール２　１０１を備える。暗号／復号化モジュール２００は、暗号化されて配信されたデータの復号化及び受信端末３内の重要なデータに対し暗号化を行ない、著作権保護等の権利、認証、課金などの処理、制御にかかわる。暗号／復号化モジュール２００については、パイレーツや暗号解読などに対するセキュリティ対策として基本的に１デバイスにより構成されるが、さらなるセキュリティ対策として、モジュールごと取りかえることが可能な構成も考えられる。センタ側９と受信端末３を結ぶ地上回線１８はコンテンツに対する課金処理、ユーザーの視聴履歴、リクエストの取得の他、コンテンツ、コンテンツに対する暗号化およびその他データに対する暗号化を解除するための情報、コンテンツに関連した情報、鍵の送信等を行なう場合などにも用いられる。

【００２４】CAモジュール１　１００及びCAモジュール２　１０１は、この受信端末３を使用するユーザーの個人認証、及びユーザーの属する家族などのグループの認証等を行う。ここでいうCAモジュール１　１００、モジュール２　１０１には、メモリ媒体のほかBSデジタル放送で使用されるICカードを使用することもある。CAモジュール１　１００については、グループの認証や伝送路暗号の復号化機能等を有し、可搬性を考慮できないため受信端末３内にその機能を内蔵させることも可能となる。またCAモジュール２　１０１は、個人認証機能等を持ち、可搬も可能であり、蓄積したコンテンツを外部機器１１などで再生する際や外部機器１１にてコンテンツの契約を行なう際に、リムーバブルメディア５と共に外部機器に接続し使用することもある。なお、CAモジュール１、２の各々の役割等については後述する。

【００２５】２．データ構成

（コンテンツの定義）図３に、サービス、イベントの関係の説明図を示す。以下に、蓄積型テレビ放送サービスにおける前述したコンテンツ、及びそれに付随するイベント、サービスの単位について説明する。まずサービスとイベントの関係について説明する。

【００２６】本蓄積型テレビ放送において、サービス３５とは放送番組の連続をさし、従来のテレビ放送におけるチャンネルと同意であり、イベントとは上記サービス３５（チャンネル）内で時間軸に対して１つ存在する放送番組をさす。例えば６：００～８：００の時間枠はイベントＡ３６、８：００～９：００の時間枠はイベントＢ３７、９：００～１３：００の時間枠ではイベントＣ３８となる。またサービス３５（チャンネル）内のある任意の時間においてイベントが存在しない場合はあるが、2つ以上のイベントが存在することはない。さらにイベントとは、本蓄積型テレビ放送サービスにおいては複数コンテンツないしは単一のコンテンツにより構成される。

【００２７】次に、図４に、イベント内のコンテンツ構成例の説明図を示す。以下に、コンテンツの構成およびそのコンテンツの単位について説明する。本蓄積型テレビ放送サービスにおいては、コンテンツとは放送サイドが意図する単位で自由に決められるものであり、それを構成する最小単位とはBSデジタル放送を例にするとリソースもしくはストリーム（PES）となる。

【００２８】具体例として複数のストリーム、リソースにより構成されるイベント２０の場合について説明する。イベント２０は、映画配信２２とデータ放送（例、料理）２３により構成されるイベントである。コンテンツの構成としては、コンテンツＡ３０～Ｅ３４を有す

る。ここでは、コンテンツＡ３０は、無料で見られるメインメニュー画面２１を構成するBML文書などのリソース類を含む。コンテンツＢ３１は、５００円の視聴料が必要な映像ストリーム２４や音声ストリーム２５で構成される映画コンテンツである。コンテンツＣ３２は、この映画コンテンツに対して追加料金２００円を払うことにより視聴可能となる字幕データストリーム２６である。コンテンツＤ３３は、上記の視聴料とは別に視聴料３００円が必要な複数リソースにより構成される料理メニュー２７、中華レシピ２８などの画面を含む料理コンテンツである。コンテンツＥ３４は、その料理コンテンツ内で追加料金１００円を払うことにより視聴可能となる単一リソースである隠し味テキスト２９である。コンテンツを放送サイドが意図する課金単位と対応させて定義することにより、従来の放送番組すなわちイベント単位あるいはチャンネルであるサービス単位の課金とは異なり、上記イベント２０のような最小課金単位が単一のストリーム（字幕データストリーム２６）、単一のリソース（隠し味テキスト２９）などの細かなコンテンツ単位課金、またそれらを組み合わせた複雑な課金を行なう放送番組を制作することが可能となる。またこのコンテンツの定義としては有料・無料の他に、著作権のあるなしなどによるコピー制御、視聴制御も含むことができる。これによりコンテンツ自体に暗号化を行なったまま蓄積媒体に保存することもある。

【００２９】（メタデータの構成）次に、図５に、コンテンツに付随する情報の構成図を示す。以下に、上記コンテンツを配信するときに必要となる情報、配信されたコンテンツを蓄積する際に必要となる情報、そのコンテンツを検索するために必要な情報、視聴もしくは視聴契約を行なうために必要な情報、暗号化されたコンテンツを復号するための情報、さらにはコンテンツを外部機器に持ち出すときに必要となる情報等、コンテンツに対し付随する情報の構成等について説明する。

【００３０】図において、蓄積型テレビ放送サービスを受信する受信端末（PDR）３内の蓄積媒体４、外部機器に持ち出す際に必要となるリムーバブルメディア５、前述した通り個人を認証する際や外部機器にコンテンツを持ち出す際に必要となるCAモジュール２　１０１（ここではその物理的媒体を可搬性に富んだ「ICカード　２」として説明する。）が示される。ICカード２は、受信端末３に登録されているユーザー数と同じだけの枚数が存在する、本例ではその登録ユーザー数をa、bの２ユーザーとし、ICカード２(a)用８０、ICカード２(b)用８１の2枚が存在するものとし説明する。蓄積型テレビ放送サービスでは、放送サイドはコンテンツに対し著作権、コピー制御、検索用の情報、視聴料などの課金に関する情報、配信するコンテンツが暗号化されている場合はその暗号を解除するための情報等（暗号化で使用された鍵、もしくは鍵のある場所や、その暗号方式を指定する情報等）の様々な情報をコンテンツ１に対し添付して配信するが、そのようなコンテンツに関する情報を本発明では「メタデータ５０」と呼ぶ。

【００３１】受信端末（PDR）３では、配信されてきたコンテンツ１、メタデータ５０をCAモジュール１　１００の契約情報等により随時蓄積媒体４に蓄積するか、もしくは復号化及び暗号化が必要であれば受信端末３内の暗号／復号化モジュール２００にて処理など必要に応じて一部加工後、蓄積媒体４に蓄積する。さらにこの例では、メタデータ５０は、配信されてきた状態では不完全な状態の場合もあり、別途配信されるBSデジタル放送ではPSI／SI（Program Specific Information/Service Information,番組特定情報/番組配列情報）と呼ばれる番組配列情報より必要な情報を取得し追記する場合もある。このメタデータ５０は、メタデータＡ～Ｃを含み、例えば、メタデータA５７のように少なくともコンテンツA５６に対しひとつ配信され、蓄積媒体４内に蓄積される。また、前述したイベント２０のような複雑なコンテンツ構成の場合、受信端末の検索、課金処理などを容易にするために、メタデータX５８のように複数のコンテンツにまたがるようなメタデータX５８を配信、蓄積することによりメタデータ５０が階層化される場合もある。メタデータ１　５２及び２　５１、５９は、例えば、コンテンツＡ５６に対しひとつ存在するメタデータＡ５７を元に、各ユーザーの視聴契約が行なわれる際に生成され、分新化される。また、複数ユーザーにより視聴契約が行なわれた場合には、メタデータ２A(a)５１、メタデータ２A(b)５９のように複数存在する。逆に視聴契約が行なわれない場合は存在しない場合もある。

【００３２】メタデータ１A(a)５２、メタデータ２A(a)５１は、例えば、ユーザーが実際に蓄積されたコンテンツＡ５６に対し視聴契約を行なった際に、メタデータＡ５７にコンテンツＡ５６が暗号化されている場合はそれに付随する情報、視聴契約の契約内容等の情報を追記し分割することにより生成される情報である。メタデータ１A(a)５２は個人認証用のCAモジュール２　１０１（本例ではユーザー(a)による視聴契約の場合であるためICカード２(a)用８０）に埋め込まれ、メタデータ２A(a)５１はコンテンツＡ５６が蓄積されている蓄積媒体４内に保存される。またコンテンツＡ５６を外部機器に持ち出すためにリムーバブルメディア５に移す、ないしはコピーする場合も、同じくそのコンテンツＡ５６に伴うメタデータ２A(a)５１をリムーバブルメディア５に書込む。メタデータ１A(a)５２も同じくICカード２(a)用８０に書込まれる。

【００３３】受信端末３内部では、検索処理を向上させるために階層化されたメタデータに含まれる情報を吸い上げ、検索用テーブル５５を生成する。この検索用テーブル５５は、ユーザーが直接触れられるものではなく、ユーザーが検索などを行なう場合には、受信端末３内の

アプリケーションプログラムからプロファイル５３、５４を介し検索用テーブル５５を利用し、該コンテンツの検索を行なう。この際使用可能なプロファイルを識別するためのパスワード入力などの個人認証が行なわれる。本蓄積型テレビ放送サービスにおけるプロファイルとは放送サイドより配信されるものではなく、予め受信端末３内に存在しユーザーの視聴契約情報すなわち蓄積媒体内のメタデータ２とCAモジュール２　１０１内のメタデータ１より常に更新されるものである。このプロファイルには、個人契約にかかわるユーザー個人に対する個人用のプロファイル５４と、各ユーザー間の相互関係などのグループ契約にかかわる全体プロファイル５３が存在する。個人用プロファイルには受信端末３に登録されていないユーザーのためのゲスト用プロファイルも存在する。このプロファイル５３、５４と検索用テーブル５５とのやりとりにより、ユーザーは蓄積媒体内に蓄積されているコンテンツに対してユーザー自身が利用可能なコンテンツの検索が可能となる。さらにプロファイルとしてはユーザーの視聴するコンテンツのジャンル等の履歴を保持し、それによりユーザー嗜好性に沿った自動コンテンツ蓄積などを実現する。以上が本蓄積型テレビ放送サービスにおけるコンテンツに付随する情報の構成である。

【００３４】（配信データの構成）次に、図６に、配信時のデータ構成図を示す。以下に、コンテンツとそれに付随する情報を配信する際のデータ構成について説明する。

【００３５】配信する際のデータ構成は、インフラとしてBSデジタル放送を利用する場合、データ放送コンテンツについてはDSM-CC伝送方式であるデータカルーセルにより伝送し、映像・音声・字幕などのストリームはPES伝送方式を利用する。以下に、前述したイベント２０のコンテンツ構成の場合を例とし配信データの構成を説明する。本蓄積型テレビ放送サービスにおける配信時のデータ構成としては、デフォルトES０　６０、映像・音声・データ･ストリーム　ES１　６１、ＥＳ２６２　ES３　６３、データカルーセルES４　６４、PSI／SI６５等に分けられる。ES０　６０は、受信端末３のデータ取得処理を向上させるためコンテンツの構成などの記載されたメタデータX５８、メタデータＡ５７などのメタデータを集め１つのESとしたデフォルトESである。ES１～４　６１、６２、６３、６４は、各種コンテンツを伝送するコンテンツ伝送用ESである。PSI／SI６５は、これらのES群の構成、もしくはサービスの視聴契約、イベントの視聴契約、EPG生成用情報を含む。イベント２０の場合、コンテンツＢ、コンテンツＣのような映像ストリーム、音声ストリーム、データストリームといったPES伝送方式に依存するコンテンツはそれぞれ単体でES1　６１、ES2　６２、ES3　６３、のようにESを構成する。一方データ放送コンテンツであるコンテンツＡ、コンテンツＤ、コンテンツＥなどのカルーセル伝送方式に依存するコンテンツは、PESの場合と同様に単体でESを構成することも可能だが基本的にはデータ伝送効率を考慮し、ES４６４のように複数コンテンツによりＥＳを構成し伝送される。またこの複数コンテンツにより構成されるESが複数ESとなる場合もある。

【００３６】３．暗号化・複号化

（暗号方式）本発明で示す総合データ配信サービスの暗号方式には著作権保護暗号方式と限定受信方式がある。

【００３７】図２３に、送信側において暗号化されたコンテンツ、メタデータの暗号形態の説明図を示す。まず、コンテンツ、メタデータの制作終了の時点で、コンテンツをファイルもしくはストリーム単位で著作権保護暗号で鍵Kk　１１０を用いて暗号化する。その鍵をメタデータに埋め込み１１１メタデータファイルを著作権保護暗号で鍵Kwc　１１２を用いて暗号化する。それら暗号化コンテンツ、暗号化メタデータの伝送形態であるMPEG-２ TSを鍵Ks　１１３で暗号化する。

【００３８】（コンテンツ暗号化方式）次に、図７に、蓄積型テレビ放送サービスにおける暗号化方式の説明図を示す。インフラであるBSデジタル放送の伝送路における伝送データ暗号化（Multi2暗号化方式）以外に、本発明では、コンテンツ自体に暗号化を行ない、暗号化したコンテンツを蓄積媒体に蓄積する。このような本発明で使用する本蓄積型テレビ放送サービス特有の暗号化方式（ここではK暗号と呼ぶ）について以下に、説明する。コンテンツ暗号方式は、伝送路の暗号化方式とは異なり、配信用データの組み立て後ではなくコンテンツの制作完了時に暗号化を行なう。コンテンツとは前述の通り放送サイドが意図する単位であるため、それを構成するリソース、ストリームなどの組み合わせも様々になる。よってここではその代表的な組み合わせを例に説明する。

【００３９】例えば、コンテンツＡ３０は、前述したイベント２０のコンテンツＡのように複数のBML文書などのリソースにより構成されるコンテンツである。コンテンツＢ３１は、同様にイベント２０におけるコンテンツＢのように複数ストリームにより構成されるコンテンツである。コンテンツＥ３４は、単一リソース、コンテンツＣ３２は、単一ストリームで構成されるコンテンツである。コンテンツ暗号方式では、これら様々な構成によるコンテンツのいずれの場合も同様に暗号化を行うため、各リソース、ストリームを単に始まりと終わりのあるデータの塊としてとらえ、暗号化処理部７０にてそれらのデータの塊を固定長ブロックに分け、ブロック毎に順番に暗号化を行なうものとする。この方式により、暗号化するデータのフォーマットであるリソース、ストリームの区別のない暗号化が可能となる。但し、暗号化処理部７０より出力される暗号化された暗号化データ（リソース）７１、暗号化データ（ストリーム）７２は元の

データフォーマットであるリソース、ストリームの区別が出来なくなるため、生成される暗号化情報７３は、例えば、別途その暗号化データ７１、７２の元のデータフォーマット、リソースの形式、各暗号化データ間の相互関係であるコンテンツ内の構成、暗号化を行なう際に使用した鍵、あるいは暗号方式を複数運用する場合は、掛けられている暗号方式の指定などの復号時に必要となる情報などを含む。放送サイドではこの暗号化情報７３を元に暗号化データ（リソース）７１はカルーセル化、暗号化データ（ストリーム）７２はPES化し、前述の配信データ構成のようなデータ構成に組み立てる。さらにこの暗号化情報７３は番組配列情報であるPSI／SIないしはメタデータ５０を生成する際にも反映される。またこのコンテンツに対する暗号化を行なう際に使用する鍵を本蓄積型テレビ放送サービスではコンテンツ鍵Kkと呼ぶ。コンテンツ鍵Kkは運用条件により1種類での運用、コンテンツ毎にユニークでの運用など様々な運用が可能である。

【００４０】（鍵配信方式）まず、映像ストリームの伝送について説明する。一般に、映像ストリームは、固定長のデータにブロック化される。各ブロックにはヘッダ情報が追加される。TSP（Transport Stream Packet）は、このヘッダとデータの組であり、伝送時のデータパケットのフォーマットを指す。既存型でスクランブル（暗号）を掛ける場合はデータ部分を暗号化する。ECM（Entitlement Control Message）は、ユーザー全体に共通的に伝送される情報であり、番組情報および制御情報を含む共通情報の伝送メッセージである。番組情報とは、例えば、番組に関する情報とデスクランブルのための鍵などであり、制御情報とは、例えば、デコーダのデスクランブル機能の強制オン／オフの指令などである。ECMは、基本的にコンテンツのスクランブル鍵を伝送するため、コンテンツと共に伝送されるものであり、ある特定ユーザーに限定して送られる情報ではない。また、EMM（Entitlement Management Message）は、加入者毎の契約情報および共通情報の暗号を解くためのワーク鍵を含む個別情報の伝送メッセージである。EMMは、基本的にユーザーが契約した事業者の鍵等を送るため、ある特定ユーザーを限定して送られる情報である。また、CA（Conditional Access）systemとは、限定受信方式を指し、サービス（編成チャンネル）やイベント（番組）の視聴を暗号化鍵で制御するシステムである。

【００４１】次に、図８に、伝送路暗号とコンテンツ、メタデータ暗号の関係の説明図を示す。以下に、BSデジタル放送と本サービスにおける、暗号化データ及び鍵の配信方法について説明する。図には、BS伝送路暗号３０３と、コンテンツ、メタデータ暗号３０１、３０２の関係が示される。コンテンツ、メタデータ暗号３０１、３０２はコンテンツ１やメタデータ５０のデータを直接暗号化するのに対して、BS伝送路暗号３０３はコンテンツ、メタデータ等を含んだイベントの伝送形態であるTSP３００に対して暗号化する。

【００４２】（BS伝送路暗号）図９に、伝送路における鍵配信方式の説明図を示す。以下に、BS伝送路暗号３０３の暗号化データ及び鍵の伝送方法を説明する。まず、コンテンツ１、メタデータ５０等を含んだイベント２０の伝送形態であるTSP３００に対して、スクランブル鍵Ks３１０で暗号化３１１する。次にスクランブル鍵Ks３１０をワーク鍵Kwl　３１３で暗号化３１４し、Ks'３１５を作成する。この時のワーク鍵Kwl３１３は放送サイドの事業者毎に定めている鍵であって、本サービスの視聴可、不可に関わる鍵である。最後に、ワーク鍵Kwl３１３を各受信端末（PDR）毎に一意である個人鍵Kml３１６で暗号化３１７し、Kwl'３１８を作成する。これら、暗号化されたデータ及び鍵を、暗号化イベントデータ３１２はBS伝送路、Ks'３１５はECM３１９、Kwl'３１８はEMM３２０を用いて伝送する。それら暗号化データを受信した受信端末（PDR）はCAモジュール１００内に格納されている個人鍵Kml　３１６を用いて復号する。まず、EMM３２０で伝送されたKwl'　３１８を個人鍵Kml　３１６を用いて復号３２１し、ワーク鍵Kwl　３１３を入手する。次に、ECM３１９を用いて伝送されたKs'　３１５をワーク鍵Kwl　３１３を用いて復号３２２し、スクランブル鍵Ks　３１０を入手する。最後に、BS伝送路を用いて伝送された暗号化イベントデータ３１２をスクランブル鍵Ks３１０を用いて復号３２３し、イベントの伝送形態であるTSPを入手する。

【００４３】（コンテンツ、メタデータ暗号）以下に、コンテンツ鍵伝送モデルについて、ECMを用いた場合、及びメタデータを用いた場合の各々について説明する。

【００４４】（ECMを用いたコンテンツ鍵伝送モデル）まず、コンテンツ鍵Kk３３０をECM３１９を用いて伝送する場合のコンテンツ１、メタデータ５０の伝送方法を説明する。

【００４５】図１０に、ECMを用いたコンテンツ鍵伝送モデルの説明図を示す。以下に、コンテンツ伝送について説明する。まず、コンテンツ１をコンテンツ鍵Kk３３０で暗号化３３１する。次にコンテンツ鍵Kk３３０をワーク鍵Kwc３３３で暗号化３３４し、Kk'３３５を作成する。このワーク鍵Kwc３３３は放送サイドの各事業者毎に定めている鍵である。この鍵は、BS伝送路暗号で用いられる鍵Kwl　３１３を共用する事も可能である。最後に、ワーク鍵Kwc３３３を各受信端末（PDR）もしくは受信端末（PDR）内の暗号／復号化モジュール毎に一意である鍵Kmc３３６で暗号化３３７し、Kwc'３３８を作成する。鍵Kmc３３６は全ての受信端末（PDR）において1種類にする事も可能である。これら、暗号化されたデータ及び鍵を、暗号化コンテンツはBS伝送路、Kk'３３５はECM３１９、Kwc'３３８はEMM３２０を用いて伝送する。それら暗号化データを受信した受信端末（PDR）は

受信端末（PDR）内に格納されている鍵Kmc３３６を用いて復号する。まず、EMM３２０で伝送されたKwc'３３８を鍵Kmc３３６を用いて復号３３９し、ワーク鍵Kwc３３３を入手する。鍵Kwc３３３は一度受信端末（PDR）に伝送されると更新されるまで受信端末（PDR）内に保持される。更新方法は、再度EMM３２０を用いてKwc'３３８を伝送し、Kmc３３６を用いて復号３３９し、新しい鍵Kwc３３３を入手する。次に、ECM３１９を用いて伝送されたKk'３３５をワーク鍵Kwc３３３を用いて復号３４０し、コンテンツ鍵Kk３３０を入手する。最後に、BS伝送路を用いて伝送された暗号化コンテンツ３３２をコンテンツ鍵Kk３３０を用いて復号３４１し、コンテンツ１を入手する。

【００４６】図１１に、メタデータの伝送モデルの説明図を示す。以下に、メタデータ伝送について説明する。まず、メタデータ５０をワーク鍵Kwc３３３で暗号化３５０する。この時のワーク鍵Kwc３３３はBS伝送路暗号で用いられる鍵Kwl３１３を用いる事も可能である。次に、ワーク鍵Kwc３３３を各受信端末（PDR）毎に一意である鍵Kmc３３６で暗号化３３７し、Kwc'３３８を作成する。これら、暗号化されたデータ及び鍵を、暗号化メタデータ３５１はBS伝送路、Kwc'３３８はEMM３２０を用いて伝送する。それら暗号化データを受信した受信端末（PDR）は受信端末（PDR）内に格納されている鍵Kmc３３６を用いて復号する。まず、EMM３２０で伝送されたKwc'３３８を鍵Kmc３３６を用いて復号３３９し、ワーク鍵Kwc３３３を入手する。次に、BS伝送路を用いて伝送された暗号化メタデータ３５１をワーク鍵Kwc３３３を用いて復号３５２し、メタデータ５０を入手する。最後に、BS伝送路を用いて伝送された暗号化コンテンツ３３２をメタデータ５０に記入されているコンテンツ鍵Kk３３０を用いて復号し、コンテンツ１を入手する。

【００４７】（メタデータを用いたコンテンツ鍵伝送モデル）図１２に、メタデータを用いたコンテンツ鍵伝送モデルの説明図を示す。以下に、コンテンツ鍵Kk３３０をメタデータ５０を用いて伝送する場合のコンテンツ１、メタデータ５０の伝送方法を説明する。まず、コンテンツ１をコンテンツ鍵Kk３３０で暗号化３３１する。そのコンテンツ鍵Kk３３０をメタデータ５０に追記し、メタデータ５０をワーク鍵Kwc３３３で暗号化３５０する。この時のワーク鍵Kwc３３３はBS伝送路暗号で用いられる鍵Kwl　３１３を用いる事も可能である。最後に、ワーク鍵Kwc３３３を各受信端末（PDR）毎に一意である鍵Kmc３３６で暗号化３３７し、Kwc'３３８を作成する。これら、暗号化されたデータ及び鍵を、暗号化コンテンツ３３２、暗号化メタデータ３５１はBS伝送路、Kwc'３３８はEMM３２０を用いて伝送する。それら暗号化データを受信した受信端末（PDR）は受信端末（PDR）内に格納されている鍵Kmc３３６を用いて復号する。まず、EMM３２０で伝送されたKwc'３３８を鍵Kmc３３６を用いて復号３３９し、ワーク鍵Kwc３３３を入手する。次に、BS伝送路を用いて伝送された暗号化メタデータ３５１をワーク鍵Kwc３３３を用いて復号３５２し、メタデータ５０を入手する。最後に、BS伝送路を用いて伝送された暗号化コンテンツ３３２をメタデータ５０に記入されているコンテンツ鍵Kk３３０を用いて復号し、コンテンツ１を入手する。

【００４８】（拡張モデル）上記の２つのモデルにおいては、コンテンツ鍵Kk３３０はコンテンツとセットで伝送している。それ以外に、拡張モデルとして、上記２つのモデルでコンテンツ鍵Kk３３０を伝送しているECM３１９またはメタデータ５０では、コンテンツ鍵Kk３３０を記入せずに、コンテンツ鍵Kk３３０の所在を示すURl、鍵ID等の情報のみを記入し、コンテンツとセットで伝送することも可能である。その際のコンテンツ鍵Kk３３０の所在として、鍵管理センタ、受信端末（PDR）内RAM、HDD等が想定される。鍵入手方法として、地上回線、衛星回線等を用いて鍵管理センタから鍵を入手する方法や、前もって地上回線、衛星回線等を用いて受信端末（PDR）内のRAMに対して全ての鍵を配信しておき、必要に応じて鍵を入手する方法や、地上回線、衛星回線等を用いて、コンテンツ１、メタデータ５０とは別に、鍵ファイルとして配信してHDDに蓄積し、必要に応じて入手する方法が可能である。

【００４９】（鍵管理）ECM３１９を用いたコンテンツ鍵伝送モデル、メタデータ５０を用いたコンテンツ鍵伝送モデルのどちらとも、受信端末（PDR）内ではコンテンツ鍵Kk３３０はコンテンツとセットであるメタデータに記入されている。よって、コンテンツ鍵Kk３３０はコンテンツ１毎に変更可能である。つまり、全てのコンテンツ１を1つの鍵で管理したり、全てのコンテンツ１に異なる鍵を用いる事もでき、幅広い鍵管理方法が可能である。

【００５０】４．受信端末

（受信端末の構成）図１３に、受信端末の構成図を示す。次に本蓄積型テレビ放送サービスを受信するのに必要な受信端末３内の構成を説明する。受信端末３は、アンテナ２を介しコンテンツ・メタデータ・番組配列情報PSI／SIなどの各種データを受信する受信モジュール１２、受信したコンテンツなどのデータを蓄積する蓄積媒体４、リムーバブルメディア５とのI／Fであるリムーバブルメディア用ドライブ１６、契約情報等の個人ないしはグループの情報が書き込まれているCAモジュール１１００及びCAモジュール２　１０１、コンテンツをTV１７等のモニタ装置で表示・再生させるためのデコーダ１５、暗号／復号化モジュール２００、各処理にかかわるCPU１３、メモリ１４を備える。リムーバブルメディア５は、蓄積したコンテンツを外部機器で使用するために必要なものである。

【００５１】受信モジュール１２は、受信したデータの中でユーザーが選択したサービスに必要となるデータのみを抽出する機能や、CAモジュール１　１００を利用することにより前述した伝送路におけるBS暗号方式である

Mulli2暗号を解除するデスクランブル機能を持つ。蓄積媒体４ないしリムーバブルメディア５に受信モジュール１２で受信したコンテンツを蓄積する際のコンテンツの蓄積形態は、上記の伝送路の暗号が解かれた形態で蓄積される。そのため、蓄積されるコンテンツ１は、本蓄積型テレビ放送サービス用の暗号が掛けられた暗号あり、リソース３９、暗号ありストリーム４１、暗号化がされていない暗号なしリソース４０、暗号なしストリーム４２の組み合わせにより構成される。一方蓄積媒体４にコンテンツと共に蓄積されるメタデータは、伝送時の暗号を暗号／復号化モジュール２００にて一度復号し、その後再び暗号／復号化モジュール２００内で生成もしくは用意される使い捨て鍵Kiにより暗号化され蓄積媒体４に蓄積される。

【００５２】さらに、暗号／復号化モジュール２００は、受信端末３内でのデータの暗号化、復号化、その他権利、認証、課金等の処理、制御に関わる。詳細には、暗号／復号化モジュール２００では、ユーザーの視聴契約の際に蓄積媒体4内に蓄積されたメタデータ（Kiで暗号化されている）を復号し、メタデータ１、２を生成する機能、使い捨て鍵Ki'にて再び暗号化を行ない、蓄積媒体４内にメタデータ２を、CAモジュール２にメタデータ１と共に鍵Ki'もしくは鍵に関する情報を伝送する機能を持つ。この際に使用される暗号化方式はコンテンツに対する暗号化方式とは異なるため、使い捨て鍵Ki、Ki'はコンテンツに対して使用した鍵Kkと同じものを使用することも可能である。暗号／復号化モジュール２００は、暗号化、復号化、使い捨て鍵の生成、使い捨て鍵Kiの鍵情報の保持（不揮発性メモリ等）、鍵管理、受信端末（PDR）３内で認証が必要となる各種データの、ユーザーへの認証、著作権保護、又は課金等に関する処理、制御機能を有する。さらに、暗号／復号化モジュール２００は、蓄積媒体４、リームバブルメディア用ドライブ１６、リームバブルメディア５、CAモジュールl、2　１００、１０１、地上回線１８、IEEE1394など外部につながる外部I／F１９などのI／Fに対しての伝送路のセキュリティ保護及びこれら伝送路を用いてメタデータ等の守るべきデータの伝送の際に伝送路やデータに合わせた暗号化を行ない、セキュリティ方式を選択する機能をも有する。

【００５３】（CAモジュールの役割及び契約方式）本サービスでは、CAモジュールを2種類用意する。これより、個人単位のサービス提供及び課金等が可能である。CAモジュールとしては、ICカードやスマートメディア等が考えられる。CAモジュール１　１００は、主に、受信端末３に装着・内臓することができ、CAモジュール２　１０１とは異なり可搬性の必要でないものであり、グループ契約情報、伝送路の暗号を解くための鍵情報等の情報をもつ。CAモジュール２　１０１は、リムーバブルメディアと共に受信端末外に持ち出すため可搬性の必要な、個別契約情報、使い捨て鍵の情報等をもつ。また、暗号化コンテンツ、それに伴うメタデータをメタデータ１、２に分散化し蓄積することにより、本蓄積型テレビ放送サービスではパイレーツ、著作権侵害、不正コピーなどに対するセキュリティを高めている。

【００５４】（CAモジュール１の役割及び契約方式）CAモジュール１は各受信端末（PDR）に１ずつ用意され、可搬性を持たず、受信端末（PDR）内に常時装備される。CAモジュール１は、その特性上常に受信端末（PDR）内に保持され得るので、受信端末（PDR）と分離可能な形態であるICカード等の記録媒体以外にも、受信端末（PDR）内蔵RAM等にその機能を持たせることも可能である。また、視聴権利単位は1台の受信端末（PDR）、つまり１個のCAモジュール１に対して、家族・グループ単位とすることができる。支払対象者の単位は、受信端末（PDR）、つまり１個のCAモジュール単位１とすることができる。なお、課金対象物の単位は、各チャンネルであるサービス単位、放送番組であるイベント単位である。スクランブルがかかったサービスないしイベントはCAモジュール１の情報により、視聴可否を判別する。また、コンテンツの視聴契約方法は、事前契約等が考えられる。つまり、前もって放送サイドの事業者に対し契約意思を表示しておく必要がある。

【００５５】（CAモジュール２の役割及び契約方式）CAモジュール２は、契約した各個人に対し1ずつ用意され、可搬性を持たせている。その視聴契約単位はひとつのCAモジュール２に対して、個人単位となる。よって支払対象者の単位は個人単位とすることができる。しかし、チャンネルによってはグループ契約を設けることも考えられ、その際はグループとして登録した視聴者単位での視聴契約と課金が可能である。なお、課金対象物の単位は、各コンテンツ単位である。その際のコンテンツの最小単位は前述のとおりリソースもしくはストリームである。つまり、最小でリソース単位、ストリーム単位での課金が可能である。コンテンツの視聴契約方法は、事前契約、予約録画時契約、リアルタイム録画時契約、蓄積後視聴時契約等がある。

【００５６】５．コンテンツ蓄積・視聴

（課金処理）コンテンツ蓄積は課金処理と関連するので、まず課金処理について概説する。有料コンテンツに対して、視聴契約を行うと課金処理が行われる。課金処理はメタデータに記載されている課金情報と、ユーザーが視聴契約の際に選択、追記した、視聴期間、視聴回数等の視聴条件等の情報を基に処理が行われる。課金処理が行われると、課金処理情報が受信端末（PDR）内の履歴を保持するためのメモリと、視聴契約したコンテンツとセットのメタデータに追加で書込まれる。

【００５７】課金処理が行われるタイミングは視聴契約方法によって異なる。そのタイミングとしては、例えば、蓄積前課金処理、蓄積時課金処理、蓄積後課金処理

等がある。まず、蓄積前課金処理では、コンテンツ、メタデータがHDDに蓄積される前に課金処理が行われ、課金処理が行われないと蓄積する事ができない。つまり、コンテンツが配信される前に視聴契約が行われる時である。コンテンツの視聴契約方法として、事前契約、予約録画時契約等が想定される。また、蓄積時課金処理では、コンテンツ、メタデータがHDDに蓄積される時に課金処理が行われる。つまり、コンテンツが配信されていて、そのコンテンツを蓄積する際に視聴契約が行われる時である。コンテンツの視聴契約方法として、リアルタイム録画時契約等が想定される。また、蓄積後課金処理では、コンテンツ、メタデータがHDDに蓄積された後に課金処理が行われる。つまり、HDDに蓄積されているコンテンツに対して視聴契約が行われる時である。コンテンツの視聴契約方法として蓄積後視聴時契約等が想定される。

【００５８】（コンテンツ蓄積（HDD））ここでは、配信されたコンテンツ１、メタデータ５０を受信端末（PDR）３内HDD４又はリムーバブルメディア５に蓄積するまでの処理を説明する。なお、蓄積の際にも暗号化がなされる。ここでは、本蓄積型テレビ放送サービスにおいて、課金処理として蓄積後課金をサービスとした例として示す。なお、コンテンツ蓄積は、以下のようなECMを用いた蓄積とメタデータを用いた蓄積のうち、システム上いずれか一方の方式を採用することができる。また、両方の蓄積方法を使うことが可能なように設定することもできる。

【００５９】「(a)ECMを用いた蓄積」と「(b)メタデータを用いた蓄積」の違いは、コンテンツの鍵Kkの配信方法が異なるという点のみである。すなわち、「(a)ECMを用いた蓄積」ではECMを用いて配信するのに対し、「(b)メタデータを用いた蓄積」では配信時からメタデータに格納して配信する。しかも、「(a)ECMを用いた蓄積」の場合には、後述するようにメタデータにコンテンツの鍵Kkの格納処理を行うので、HDDに蓄積する際は、「(a)ECMを用いた蓄積」と「(b)メタデータを用いた蓄積」は全く同じ形態となる。よって、それ以降の「コンテンツ視聴」における処理手順は全く同じとなる。一方、「(c)リムーバブルメディアに蓄積」は、「(a)ECMを用いた蓄積」「(b)メタデータを用いた蓄積」のどちらかの方式を用いてHDDに蓄積されたコンテンツとメタデータを、契約手続きと課金処理終了後にリムーバブルメディアに改めて蓄積する場合である。よって、その後の「コンテンツ視聴」処理は、「(a)ECMを用いた蓄積」又は「(b)メタデータを用いた蓄積」の後の視聴の場合とは異なる。

【００６０】（a.ECMを用いたコンテンツ鍵伝送モデルにおける蓄積）図１４に、ECMを用いたコンテンツ鍵伝送方式における処理手順の説明図を示す。また、図１６に、コンテンツ鍵伝送方式における処理手順１のフローチャートを示す。以下に、ECMを用いたコンテンツ鍵伝送方式における処理手順を説明する。なお、この処理は、主に、暗号／復合化モジュール２００により実行される。また各鍵については、図９～図１２中の記号を示す。

【００６１】まず初めにKs３１０、Kwl３１３とCAモジュール１　１００に蓄積されているKml　３１６を用いて、BS伝送路スクランブルを復号し（５００）、暗号化コンテンツ４０１、暗号化メタデータ４０２を入手する。次に、予め受信端末（PDR）３に伝送され暗号/復号化モジュール２００のRAM４０３に蓄積されているワーク鍵Kwc３３３を用いて、ECM４００（３１９）を用いて伝送されたKk’３３５を復号し（５０１）、コンテンツ鍵Kk３３０を入手し（５０２）、RAM４０３に格納する。その後、暗号/復号化モジュール２００のRAM４０３に格納されているワーク鍵Kwc３３３を用いてメタデータ４０２を復号し（５０３，４０４）、メタデータに記載されている検索/課金などの検索処理に用いられる情報を抽出し検索テーブル４１０に追加する（５０４）。この検索テーブル４１０はHDD４内のコンテンツ４０６の検索/課金情報などが記載されていて、検索をする際に使用される。メタデータから検索処理に用いられる情報を抽出し検索テーブルに追記した後、メタデータ４０２にコンテンツ鍵Kk３３０を追記する（５０５，４０４）。さらに、受信端末（PDR）３内の暗号/復号化モジュール２００で生成もしくは用意させた値Kl４０４を鍵Klとして（５０６）、Kwcで一度復号されたメタデータをKlで再暗号化４０４し（５０７）、Klで暗号化されたメタデータ４０５を生成する４０４。鍵Klは暗号/復号化モジュール２００のRAM４０３に格納される。この鍵Klは、メタデータ４０２をHDD４蓄積前に復号し再暗号化４０４する度に暗号/復号化モジュール２００内で生成もしくは用意させる鍵である。その後、コンテンツ鍵Kk３３０で暗号化された暗号化コンテンツ４０６と鍵Klで暗号化された暗号化メタデータ４０５をセットでHDD４に蓄積する（５０８）。なお、メタデータ４０５毎に異なる鍵としてもよい。

【００６２】（b.メタデータを用いたコンテンツ鍵伝送モデルにおける蓄積）図１５に、メタデータを用いたコンテンツ鍵伝送方式における処理手順の説明図を示す。また、図１７に、コンテンツ鍵伝送方式における処理手順２のフローチャートを示す。以下に、メタデータ５０を用いたコンテンツ鍵伝送方式における処理手順を説明する。

【００６３】まず初めにKs３１０、Kwl　３１３とCAモジュール１　１００に蓄積されているKml　３１６を用いてBS伝送路スクランブルを復号し（５００）、暗号化コンテンツ４０１、暗号化メタデータ４５１を入手する。この場合、暗号化メタデータ４５１には、コンテンツ鍵Kkが含まれる。次に、予め受信端末（PDR）３に伝送され

暗号/復号化モジュール２００内のRAM４５２に格納されているワーク鍵Kwc３３３を用いてメタデータ４５１を復号し（５０３，４５３）、メタデータに記載されている検索/課金情報などの検索処理に用いられる情報を抽出し検索テーブル４１０に追加する（５０４）。この検索テーブル４１０はHDD４内のコンテンツ４０６の検索/課金情報が記載されていて、検索をする際に使用される。メタデータから検索処理に用いられる情報を抽出し検索テーブルに追記した後、暗号/復号化モジュール２００内で生成もしくは用意させた値Kiを鍵Ki４５３として（５０６）、Kwcで一度復号されたメタデータをKiで再暗号化４５３し（５０７）、Kiで暗号化されたメタデータ４０５を生成する（４５３）。鍵Kiは暗号/復号化モジュール２００内のRAM４５２に格納される。この鍵Kiは、メタデータ４５１をHDD４蓄積前に復号し再暗号化４５３する度に暗号/復号化モジュール２００内で生成もしくは用意させる鍵である。その後、コンテンツ鍵Kk３３０で暗号化された暗号化コンテンツ４０６と鍵Kiで暗号化された暗号化メタデータ４０５をセットでHDD４に蓄積する（５０８）。なお、メタデータ４１４毎に異なる鍵としてもよい。

【００６４】（c.リムーバブルメディアへのコンテンツ蓄積）図１８に、リムーバブルメディアへのコンテンツ蓄積処理手順のフローチャートを示す。以下に、HDD４に蓄積されたコンテンツ４０６をリムーバブルメディア５に蓄積するまでの処理手順を説明する。図１４、図１５にリムーバブルメディアへのコンテンツ蓄積処理の説明図を示す（両者は同様である）。

【００６５】ユーザーがキーワード等を入力することにより、検索テーブル４１０の情報を基にHDD４内の検索処理４１２が行われる（５２０）。その検索結果より、ユーザーが蓄積コンテンツ４０９を選択する（５２０）。そして、選択されたコンテンツ４０９に対するメタデータ４０８を受信端末（PDR）３内のワークエリアにコピーする。コピーされたメタデータ４０８を鍵Kiを用いて復号４１３する（５２２）。そして、ユーザーが、選択したコンテンツ４０８の契約条件を確認後必要な情報を追記し、蓄積を決定４１５する（５２３）。ユーザーの蓄積決定の動作を受けて、ユーザーが契約した契約条件より課金処理４１６が行われる（５２４）。契約条件、課金処理の結果より、メタデータ４１４の契約情報を作成する（５２５）。その後、メタデータ４１４をメタデータ１、２に分離する（５２６）。そして、受信端末（PDR）３内で生成もしくは用意させた値Ki'を鍵Ki'４１８とする（５２７）。この鍵Ki'は、コンテンツ４０９の視聴手続き後、メタデータ２をリムーバブルメディア５、HDD４等に蓄積前に暗号化する度に受信端末（PDR）３内で生成もしくは用意させる鍵である。メタデータ２を鍵Ki'で暗号化し（５２８）、リムーバブルメディア５に蓄積する（５２９）。次に、メタデータ１に鍵Ki'もしくは、鍵に関する情報を記入する。メタデータ１をセキュリティが守られている伝送路を用いてCAモジュール２　１０１に蓄積し（５３１）、CAモジュール２　１０１に蓄積されている個人鍵Km2　４２４を用いて暗号化４２２する（５３０）。この処理において、セキュリティが守られている伝送路を用いて個人鍵Km2　４２４を受信端末（PDR）３内に入力し、鍵Ki'もしくは鍵Ki'に関する情報を含んでいるメタデータ１を個人鍵Km2　４２４を用いて暗号化した（４２２、５３０）後、CAモジュール２　１０１に蓄積する（５３１）事も可能である。またこれ以外の方法として、セキュリティが守られた伝送路で鍵Ki'もしくは鍵Ki'に関する情報を含んでいるメタデータ１をCAモジュール２１０１に伝送し、そのまま保存する場合もある。メタデータ４１４に関する処理が全て完了したら、暗号化コンテンツ４０９をリムーバブルメディア５に蓄積する（５３２）。

【００６６】このようにして、リムーバブルメディアに格納される情報は、鍵Kk'で暗号化され鍵Kkを含むメタデータ２　４２１、鍵Kkで暗号化されたコンテンツ４２７となる。

【００６７】（コンテンツ視聴）図１９に、コンテンツ視聴処理手順のフローチャートを示す。また、図２４に、ECM又はメタデータを用いた蓄積後視聴のデータの流れについての説明図を示す。以下に、図１４（図１５）を参照して、HDD４に蓄積されたコンテンツ４０８を視聴するまでの処理手順を説明する。

【００６８】HDD４には、鍵Kkを含む暗号にメタデータと暗号化コンテンツが記帳されている。ユーザーがキーワード等を入力することにより、検索テーブル４１０の情報を基にHDD４内の検索処理４１２が行われる（５２０）。その検索結果より、ユーザーが視聴コンテンツ４０９を選択する（５４０）。そして、選択されたコンテンツ４０９に対するメタデータ４０８を受信端末（PDR）３内のワークエリアにコピーする。

【００６９】メタデータについては、次のように処理される。コピーされたメタデータ４０８を鍵Kiを用いて復号４１３する（５２２）。そして、ユーザーが、選択したコンテンツ４０９の契約条件を確認後、視聴を決定４１５する（５４１）。ユーザーの視聴決定の動作を受けて、ユーザーが確認、契約した契約条件より課金処理４１６が行われる（５２４）。契約条件、課金処理の結果より、メタデータの契約情報を作成４１７する（５２５）。その後、メタデータ４１４をメタデータ１、２に分離する（５２６）。そして、受信端末（PDR）３内で生成もしくは用意させた値Ki'を鍵Ki'とする（５２７）。この鍵Ki'は、コンテンツ４０９の視聴手続き後、メタデータ４１４をリムーバブルメディア５、HDD４等に蓄積する前に暗号化する度に受信端末（PDR）３内で生成もしくは用意させる鍵である（なお、メタデータ４１４毎に異なる鍵としてもよい）。次に、メタデー

タ２を鍵Kt'で暗号化４１９し（５２８）、HDDに蓄積する（５４２）。次に、セキュリティが守られている伝送路を用いて個人鍵Km2　４２４を受信端末（PDR）３内に入力し、鍵Kt'もしくは鍵Kt'に関する情報を含むメタデータ１を個人鍵Km2　４２４を用いて暗号化４２２した（５３０）後、CAモジュール２　１０１に蓄積する（５３１）。この処理において、メタデータ１に鍵Kt'もしくは鍵Kt'に関する情報を記入する。メタデータ１をセキュリティが守られている伝送路を用いてCAモジュール２　１０１に蓄積し（５３１）、CAモジュール２　１０１に蓄積されている個人鍵Km2　４２４を用いて暗号化４２２する（５３０）。またこれ以外の方法として、セキュリティが守られた伝送路で鍵Kt'もしくは鍵Kt'に関する情報を含むメタデータ１をCAモジュール2　１０１に伝送し、そのまま保存する場合もある。一方、コンテンツについては、次のように処理される。メタデータ４１４に関する処理が全て完了したら、コンテンツ鍵Kk３３０を用いて暗号化コンテンツ４０９を復号４２６し（５４３）、視聴可能なコンテンツを入手する。

【００７０】つぎに、図２５に、リムーバブルメディアに蓄積後視聴のデータの流れについての説明図を示す。リームバブルメディア５からの視聴処理についてもこのHDD４からのコンテンツの視聴処理と同様な処理が行なわれる。ただし、ここでは、ＣＡモジュール２　１０１に蓄積されたメタデータ１と、リムーバブルメディア５の蓄積されたメタデータ２との一致確認及び契約条件確認が行われた後、コンテンツの視聴（復号）が可能となる。暗号化メタデータ１は、セキュリティが守られている伝送路を用いて個人鍵Km2　４２４を受信端末３内に入力し復号することができる。復号化されたメタデータ1内の鍵Kt'を用いて、暗号化メタデータ２が復号化されることができる。メタデータ２内に格納されているコンテンツ鍵Kkにより、暗号化コンテンツを復号し、視聴可能となる。

【００７１】６．拡張サービス

次に本蓄積型テレビ放送サービスにおいてリムーバブルメディアを利用したサービス（コンテンツの外部での使用）の拡張サービスとしての第３者への譲渡を目的としたギフトサービスについて、概要を説明する。

【００７２】図２０に、通常サービスの説明図を示す。これは、前述したとおり、ユーザー６００が視聴契約を行なったコンテンツを、視聴契約を行なった受信端末（PDR）３の外部で利用する場合である。受信端末（PDR）３から持ち出す形態は、メタデータ１の書込まれたCAモジュール２　１０１と、メタデータ２及び暗号化コンテンツが書込まれたリムーバブルメディア５である。通常サービスでは、外部受信端末（PDR）６０４、もしくは外部機器１１で利用する場合にその両者を挿入あるいは接続し、ユーザー６００の持つ視聴契約の権利（個人認証など）、すなわちCAモジュール２　１０１のメタデータ１、リムーバブルメディア５のメタデータ２に基づきコンテンツの視聴が可能となる。

【００７３】図２１に、ギフトサービスの説明図を示す。ギフトサービスでは、ユーザー６００である送り主６０１が、ギフト目的の視聴契約を行なった際に生成されるメタデータのみに基づくのではなく、受け取り主６０２側でコンテンツに対する認証およびその他必要な情報が視聴契約の際にリムーバブルメディア５に書込まれ、その後視聴可能となる。この場合送り主６０１側の受信端末（PDR）３では送り主のCAモジュール２　１０１で一度視聴契約を行ない、その際に生成されたメタデータに対し必要な部分に暗号化を行ないコンテンツの書き込まれたリムーバブルメディア５に書込み受け渡す。一方、受け取り主６０２側の受信端末（PDR）６０４では、暗号化メタデータを復号し、受け取り主のCAモジュール２　６０４を使用し必要な視聴契約を行ない初めてコンテンツの視聴に必要なメタデータ１、２が生成され、コンテンツの視聴が可能となる。そのため個人の認証機能を持つCAモジュール２（送り主側の）をコンテンツと共に受け渡す必要がなくなる。この際にコンテンツなどの受け渡しの伝送路６０３は、リムーバブルメディアなどの蓄積媒体を介す手渡しや配送などのほかに、コンテンツなどのデータを放送波などの電波、地上回線などの通信線を利用し受け渡すことも可能である。

【００７４】また、メタデータに対する暗号化は通常サービスと同様に暗号／復号化モジュール内で行なわれ、その際に使用される鍵は暗号／復号化モジュールで生成もしくは用意されたものを使用する。この際に使用する鍵をギフト鍵と呼ぶ。ギフト鍵は通常サービスと同様に生成もしくは用意された鍵Kt、Kt'を使用することも可能である。

【００７５】図２２に、ギフトサービスの伝送路において必要な情報の説明図を示す。以下に、リムーバブルメディアに書込む場合を例に、ギフトサービスを行なう際のコンテンツの受け渡しに必要な情報を説明する。コンテンツ６０７は、前述の通常サービスと同様に暗号化されたコンテンツである。メタデータ６０６は、送り主側で行なわれた視聴契約により作成されたメタデータの暗号化された部分であり暗号化されたコンテンツ６０７を復号するための鍵Kkもしくは鍵に関する情報、検索／課金情報などを含んでいる。ギフト情報６０５は、メタデータの暗号化されていない部分であり、通常サービスとギフトサービスを識別する情報、暗号化したメタデータを復号するための情報等を含む情報である。この情報を本例ではギフト情報と呼ぶ。メタデータ６０６については受け取り主側でコンテンツ６０７を視聴する前に受け取り主のCAモジュール２　６０４を基に必要な視聴契約処理を行なうことにより前述のメタデータ１、２となる。またこれ以外の方法としてメタデータを復号するための情報、ギフト情報、メタデータの一部などは、通常

サービスにおけるCAモジュール２内に分離したメタデータ１と同様に分離させ、別のセキュリティの守られた伝送路、例えば地上回線、センタ側などを利用し受け取り主側に受け渡すことも可能である。

【００７６】７．まとめ

本発明の特徴のいくつかを以下に例示する。

・第３者に譲渡の目的でコンテンツを購入する際に、暗号化コンテンツと暗号化されたコンテンツに関する情報（メタデータ）と第３者に対する譲渡を目的にしていることを示すギフト情報で構成されたデータの組み合わせで譲渡目的としたサービスを実現可能とするシステムを提供すること。

・前記システムにおいて、暗号化されたコンテンツに関する情報（メタデータ）は、コンテンツの暗号化の鍵とは異なる鍵を用いて暗号化されていること可能とすること。

・前記システムにおいて、コンテンツに関する情報（メタデータ）にかける暗号化のアルゴリズムとコンテンツにかけるアルゴリズムが異なること。

【００７７】・前記システムにおいて暗号化のアルゴリズムを２種類用いることで、コンテンツに関する情報（メタデータ）とコンテンツの暗号化に用いる鍵は同じ鍵を用いることも可能であり、また異なる鍵を用いることも可能となること。

・前記システムにおいて、ギフト情報内にコンテンツに関する情報（メタデータ）を暗号化している鍵に関する情報を含むこと。

・前記システムにおいて、コンテンツに関する情報（メタデータ）には、受け取り側の所持する個人認証情報、ＣＡモジュール２に通常格納される状態の情報は記入されてなく、譲渡目的の形式であるコンテンツセットを受け取ったときに、受け取り側である所有者が認識されるので、コンテンツに関する情報（メタデータ）に受け取り側を認識できる情報が初めて記入され、通常の情報形式になること。

【００７８】・受信端末における暗号化コンテンツに対する管理を行う機能では、暗号化コンテンツの著作権管理、コンテンツに関する情報（メタデータ）の暗号／復号化，守るべきコンテンツに関するデータ、守るべき情報の移動に使用する伝送路に合わせた暗号化を行い、セキュリティ方式の選択を可能とすること。

・コンテンツはコンテンツ暗号鍵Ｋｋで暗号化し、コンテンツに関する情報であるメタデータはコンテンツとは別の鍵で同様に暗号化を行い、この二つのデータの組み合わせによる構成でコンテンツに関する視聴・購入を行わせること。

・前記暗号化されたコンテンツとコンテンツに関するメタデータは衛星回線を介して衛星回線の伝送用暗号方式でさらに暗号化された後伝送されること。

【００７９】・前記コンテンツ毎にユニークな鍵ないしは同一の鍵で暗号化を行い、暗号化の鍵情報（鍵の存在場所や鍵そのもの）をメタデータに埋め込んで配信すること。

・前記暗号化されたコンテンツの鍵を、メタデータと同一の鍵で暗号化してコンテンツ配信時とは別の時間枠や、別の配信場所で配信すること。

・衛星デジタル放送におけるＣＡモジュールに対して個人を特定可能とする第２のＣＡモジュールを有し、この第２のＣＡモジュールがユーザー個人認証の役割を行うことでマルチユーザー対応とすること。

・受信端末内に暗号・復号化を行う専用モジュールを有し、この専用モジュールは暗号化されているメタデータを受信後直に伝送依存する鍵で復号化を行い、受信端末内で生成される使い捨て鍵で再度暗号化を行い受信端末にメタデータを蓄積させること。

【００８０】・ユーザーの視聴・契約の動作に伴い、前記蓄積されている暗号化メタデータを復号し必要なデータを記入後再度新規使い捨て鍵の生成を行い、新規使い捨て鍵でメタデータを暗号化し、この暗号化メタデータを受信端末内に蓄積する、このようにユーザーのコンテンツ視聴・契約毎に新規使い捨て鍵を生成し、同じコンテンツであっても異なる使い捨て鍵となること。

・前記生成された新規使い捨て鍵を、受信端末と第２のＣＡモジュール間のセキュリティ保護された伝送インタフェースを通して、第２のＣＡモジュールに格納すること。

・受信端末内の暗号／復号化モジュールにおいて、モジュールそのものがモジュール特定鍵Ｋｍｃを有し、コンテンツ暗号鍵やメタデータの伝送時暗号に用いる伝送路鍵をモジュール特定鍵で暗号化し、受信端末内の暗号／復号化モジュールにデジタル放送の伝送方式を用いて配信し、暗号・復号モジュールで伝送路鍵を取得しモジュール内に格納後、伝送路鍵の更新において再度取得しモジュール内に格納する暗号／復号化モジュールを有すること。

【００８１】・暗号化されたコンテンツを格納するときは、暗号化されたままの状態で格納し、暗号化されたコンテンツのメタデータも一緒に格納され、コンテンツの購入時にコンテンツ購入に関するデータをメタデータに記入し、メタデータはメタデータ１とメタデータ２とに分かれ、夫々のメタデータが暗号化された後、コンテンツ鍵で暗号化されたコンテンツと購入時に暗号化されたメタデータ２が受信端末内に２つセットで格納され、同様に暗号化されたメタデータ１はＣＡモジュール２に記録され、コンテンツ視聴時に分割されたメタデータを組み立てることで暗号化されたコンテンツの復号を可能とすること。

・コンテンツを暗号化しているコンテンツ鍵Ｋｋは、本システムで管理する伝送路鍵Ｋｗｃで暗号化されてコンテンツ鍵Ｋｋ'となり、さらに伝送路鍵Ｋｗｃを暗号／

復号化モジュールの鍵Ｋｍｃで暗号化しｋｗｃ'を作成、その後伝送路にてＫｋ'、Ｋｗｃ'を送信しモジュール特定鍵Ｋｍｃで解読して伝送路鍵Ｋｗｃを取得する方式において、暗号／復号化モジュール内で伝送路鍵Ｋｗｃを格納し、受信後の蓄積時とユーザー契約時に受信端末内で使い捨て鍵を生成、その使い捨て鍵と契約関連情報等、さらにデジタル放送の番組配列情報よりの組み合わせで作成すること。

・上記システムにおいて、暗号化されたコンテンツ購入時に作成されるメタデータの分割時における、暗号化されたコンテンツと一緒に蓄積させるメタデータ２は、装置内で生成される使い捨て鍵で暗号化され、残りのメタデータ１はコンテンツ鍵を書込み後同様に使い捨て鍵で暗号化して、暗号化されたコンテンツ、メタデータをリムーバブルメディアに記録すること。

【００８２】・コンテンツ個々に対する暗号化並びに課金管理を行うことが可能となる上記システムにおいて、コンテンツ毎に異なる暗号鍵を所有することで様々な伝送路よりのコンテンツ組み合わせを可能とすること。

・家庭内受信端末では受信した暗号化コンテンツを一緒に配信されてきたメタデータと同時格納し、家庭内における受信装置ではユーザーの購入時に受信したメタデータを元に有効期限等埋め込まれたメタデータの作成を行い、そのメタデータからメタデータ１、メタデータ２を作成しメタデータを受信端末で作成する使い捨て鍵を用いて暗号化し再度受信端末内に蓄積し、メタデータはユーザー特定の個人鍵Ｋｍ２で暗号化した後、ＣＡモジュール２内に格納されるシステムにおいては、メタデータ作成時に受信したメタデータを元に作成するが，メタデータはメタデータ枠として何度も利用可能なようにメタデータ枠として残しておくこと。

・上記システムにおいて、暗号化コンテンツを視聴するには、蓄積媒体内の暗号化コンテンツを複写し、この複写した暗号化コンテンツを再生する、複写使用により蓄積媒体内の暗号化コンテンツはそのままの状態で保管され、また同時にメタデータも複写して使用することで、家庭内でも受信、蓄積したコンテンツの契約を結ぶ度に視聴でき、家庭内でユーザー特定の蓄積媒体、ＩＣカード等が数種類存在しても本サービス利用が可能となること。

【００８３】

【発明の効果】本発明によると、受信端末内で生成した使い捨て鍵を用いてメタデータの作成並びに分割化を行うことで、コンテンツ毎に暗号化可能とする。また、本発明によると、個人を特定できる第２のＣＡモジュールを合わせることで個人特定のサービスが行うことができる。

【００８４】さらに、本発明によると、メタデータ内にコンテンツの所有者情報を入れずにおくことで、コンテンツの譲渡をされた方の受け取り時に初めてコンテンツ所有者を特定でき、ＣＡモジュールへの所有者情報記入が行なわれることにより、第３者への譲渡目的としたコンテンツサービスが実現可能となる。

【図面の簡単な説明】

【図１】蓄積型テレビ放送サービスの受信側の概要図。

【図２】蓄積型テレビ放送サービスシステムの全体図。

【図３】サービス、イベントの関係の説明図。

【図４】イベント内のコンテンツ構成例の説明図。

【図５】コンテンツに付随する情報の構成図。

【図６】配信時のデータ構成図。

【図７】蓄積型テレビ放送サービスにおける暗号化方式の説明図。

【図８】伝送路暗号とコンテンツ、メタデータ暗号の関係の説明図。

【図９】伝送路における鍵配信方式の説明図。

【図１０】ECMを用いたコンテンツ鍵伝送モデルの説明図。

【図１１】メタデータの伝送モデルの説明図。

【図１２】メタデータを用いたコンテンツ鍵伝送モデルの説明図。

【図１３】受信端末の構成図。

【図１４】ECMを用いたコンテンツ鍵伝送方式における処理手順の説明図。

【図１５】メタデータを用いたコンテンツ鍵伝送方式における処理手順の説明図。

【図１６】コンテンツ鍵伝送方式における処理手順１のフローチャート。

【図１７】コンテンツ鍵伝送方式における処理手順２のフローチャート。

【図１８】リムーバブルメディアへのコンテンツ蓄積処理手順のフローチャート。

【図１９】コンテンツ視聴処理手順のフローチャート。

【図２０】通常サービスの説明図。

【図２１】ギフトサービスの説明図。

【図２２】ギフトサービスの伝送路において必要な情報の説明図。

【図２３】送信側において暗号化されたコンテンツ、メタデータの暗号形態の説明図。

【図２４】ECM又はメタデータを用いた蓄積後視聴のデータの流れについての説明図。

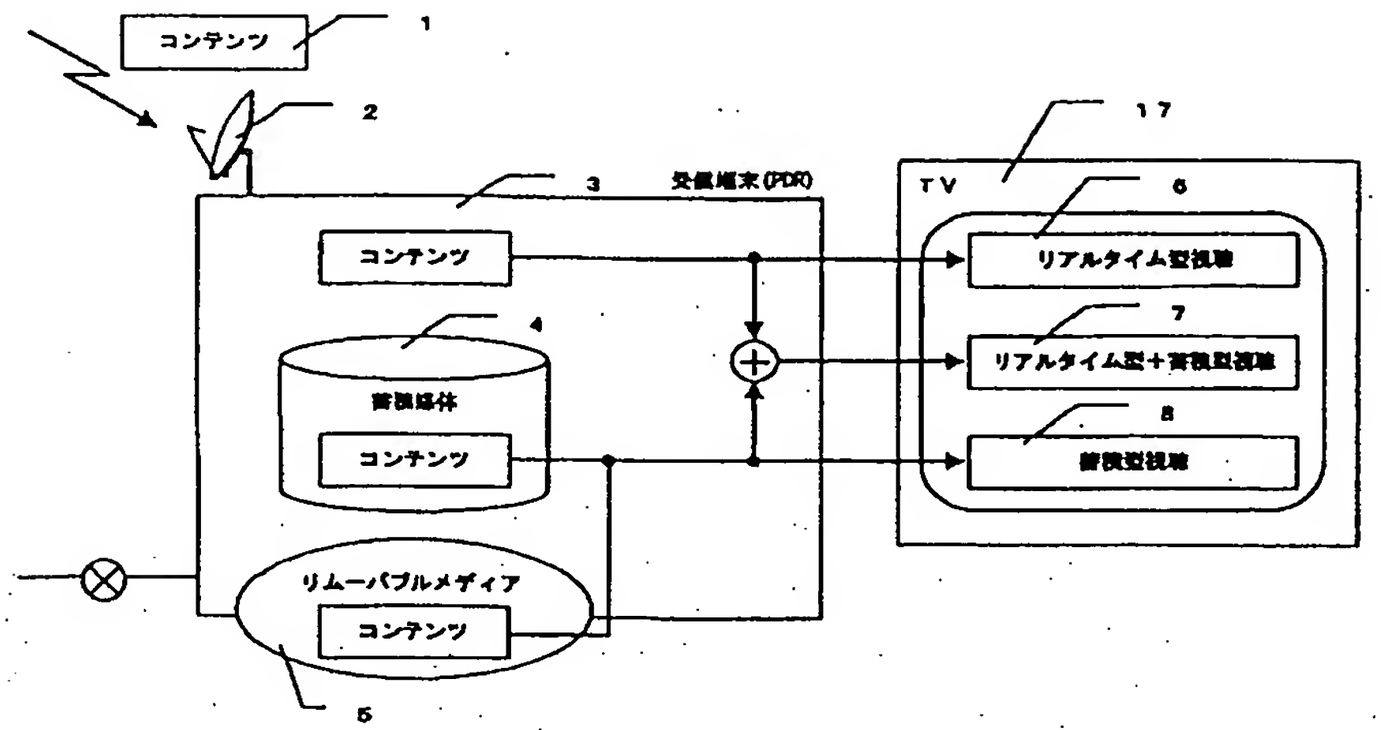
【図２５】リムーバブルメディアに蓄積後視聴のデータの流れについての説明図。

【符号の説明】

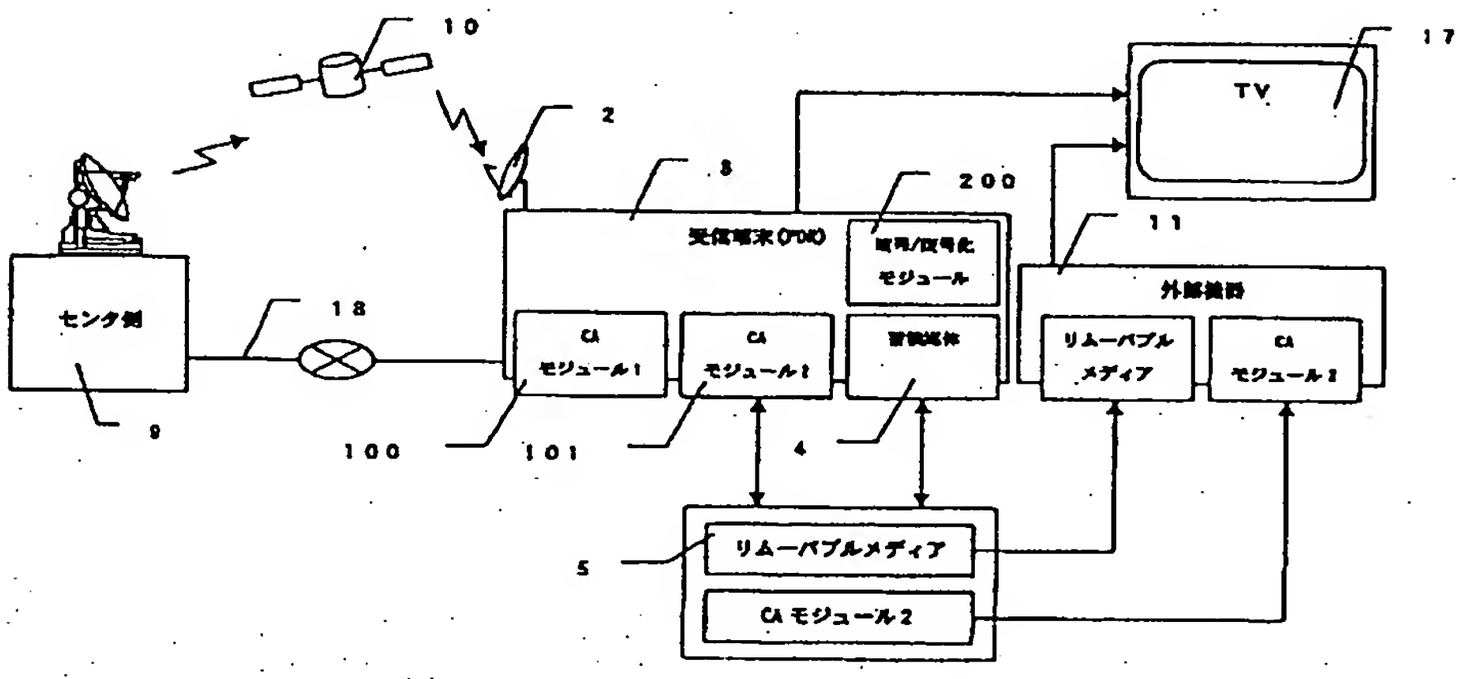
１・・・コンテンツ、２・・・アンテナ、３・・・受信端末（PDR）、４・・・蓄積媒体、５・・・リムーバブルメディア、６・・・リアルタイム型視聴、７・・・リアルタイム型＋蓄積型視聴、８・・・蓄積型視聴、９・・・センタ側（放送サイド）、１０・・・衛星、１１・・・外部機器、１２・・・受信モジュール、１３・・・CPU、１４・・・メモリ、１５・・・デコーダ、１６・

・・リムーバブルメディア用ドライブ、１７・・・ＴＶ、１８・・・地上回線、１９・・・外部I／F、２０・・・イベント、２１・・・メインメニュー画面、２２・・・映画、２３・・・料理、２４・・・映像ストリーム、２５・・・音声ストリーム、２６・・・データストリーム、２７・・・中華、２８・・・餃子写真、２９・・・隠し味、３０・・・コンテンツＡ、３１・・・コンテンツＢ、３２・・・コンテンツＣ、３３・・・コンテンツＤ、３４・・・コンテンツＥ、３５・・・サービス、３６・・・イベントＡ、３７・・・イベントＢ、３８・・・イベントＣ、３９・・・暗号ありリソース、４０・・・暗号なしリソース、４１・・・暗号ありストリーム、４２・・・暗号なしストリーム、５０・・・メタデータ、５１・・・メタデータ２A(a)、５２・・・メタデータ１A(a)、５３・・・全体プロファイル、５４・・・個人用プロファイル(a)、５５・・・検索用テーブル、５６・・・コンテンツＡ、５７・・・メタデータＡ、５８・・・メタデータＸ、５９・・・メタデータ２A(b)、６０・・・ES0（デフォルトES）、６１・・・ES1（映像ストリーム）、６２・・・ES2（音声ストリーム）、６３・・・ES3（データストリーム）、６４・・・ES4（データカルーセル）、６５・・・PSI／SI、７０・・・暗号化処理部、７１・・・暗号化データ（リソース）、７２・・・暗号化データ（ストリーム）、７３・・・暗号化情報、８０・・・ICカード２(a)用、８１・・・ICカード２(b)用、１００・・・CAモジュール１、１０１・・・CAモジュール２、２００・・・暗号／復号化モジュール、３００・・・TSP、３０１・・・コンテンツ暗号化、３０２・・・メタデータ暗号化、３０３・・・伝送路暗号化、３１０・・・Ks、３１１・・・イベント暗号化（鍵Ks）、３１２・・・暗号化イベント、３１３・・・Kw1、３１４・・・Ks暗号化（鍵Kw1）、３１５・・・Ks'、３１６・・・Km1、３１７・・・Kw1暗号化（鍵Km1）、３１８・・・Kw1'、３１９・・・ECM、３２０・・・EMM、３２１・・・Kw1'復号（鍵Km1）、３２２・・・Ks'復号（鍵Kw1）、３２３・・・暗号化イベント復号（鍵Ks）、３３０・・・Kk、３３１・・・コンテンツ暗号化（鍵Kk）、３３２・・・暗号化コンテンツ、３３３・・・Kwc、３３４・・・Kk暗号化（鍵Kwc）、３３５・・・Kk'、３３６・・・Kmc、３３７・・・Kwc暗号化（鍵Kmc）、３３８・・・Kwc'、３３９・・・Kwc'復号（鍵Kmc）、３４０・・・Kk'復号（鍵Kwc）、３４１・・・暗号化コンテンツ復号（鍵Kk）、３５０・・・メタデータ暗号化（鍵Kwc）、３５１・・・暗号化メタデータ、３５２・・・暗号化メタデータ復号（鍵Kwc）、４００・・・配信情報（ECM,EMM）、４０１・・・配信情報（コンテンツ）、４０２・・・配信情報（メタデータ）、４０３・・・RAM、４０４・・・HDD蓄積前処理、４０５・・・HDD蓄積前メタデータ、４０６・・・HDD蓄積前コンテンツ、４０７・・・HDD蓄積コンテンツ、メタデータ、４０８・・・メタデータ（コピー）、４０９・・・コンテンツ（コピー）、４１０・・・検索テーブル、４１１・・・HDD、４１２・・・検索処理、４１３・・・メタデータ復号、４１４・・・復号メタデータ、４１５・・・契約手続き、４１６・・・課金処理、４１７・・・メタデータ（契約情報）作成、４１８・・・メタデータ分離処理、４１９・・・メタデータ２暗号化、４２０・・・メタデータ２（HDD内）、４２１・・・メタデータ２（リムーバブルメディア内）、４２２・・・メタデータ１、Kt'暗号化、４２４・・・Km2、４２５・・・暗号化メタデータ、Kt,'、４５０・・・配信情報（EMM）、４５１・・・配信情報（メタデータ）、４５２・・・RAM、４５３・・・HDD蓄積前処理、５００・・・スクランブル復号、５０１・・・Kk'復号、５０２・・・Kk入手、５０３・・・メタデータ復号、５０４・・・検索テーブル情報追加、５０５・・・メタデータKk記入、５０６・・・Kt生成、５０７・・・メタデータ暗号化、５０８・・・コンテンツ、メタデータ蓄積、５２０・・・HDD検索、５２１・・・蓄積コンテンツ選択、５２２・・・メタデータ復号、５２３・・・契約条件確認・記入、蓄積選択、５２４・・・課金処理、５２５・・・契約情報作成、５２６・・・メタデータ分離、５２７・・・Kt'生成、５２８・・・メタデータ２暗号化、５２９・・・リムーバブルメディア蓄積処理（メタデータ２）、５３０・・・メタデータ１、Kt'暗号化、５３１・・・CAモジュール蓄積、５３２・・・リムーバブルメディアにコンテンツ蓄積、５４０・・・視聴コンテンツ選択、５４１・・・契約条件確認・記入、視聴選択、５４２・・・HDD蓄積、５４３・・・コンテンツ復号、６００・・・ユーザー、６０１・・・送り主、６０２・・・受け取り主、６０３・・・伝送路、６０４・・・受け取り主側CAモジュール２、６０５・・・ギフト情報、６０６・・・メタデータ、６０７・・・暗号化コンテンツ。

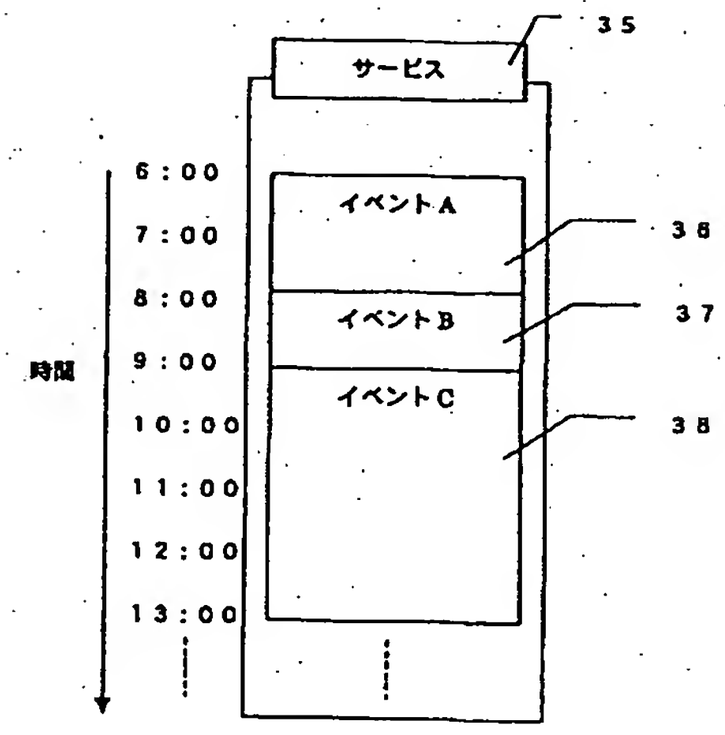
【図１】



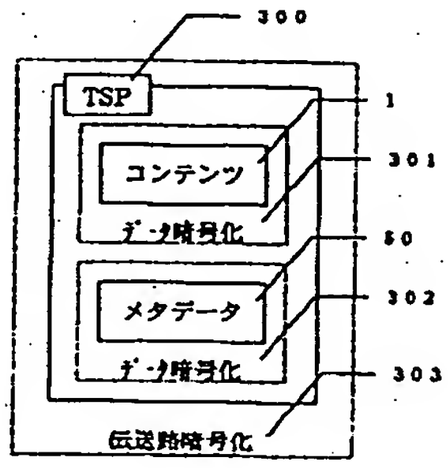
【図２】



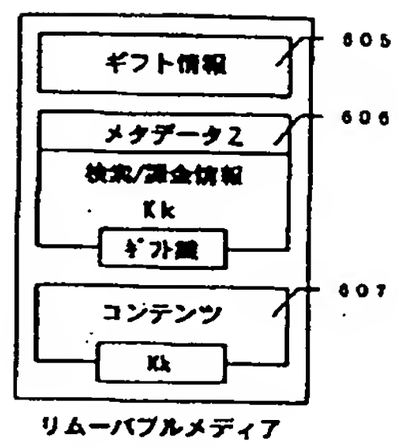
【図３】



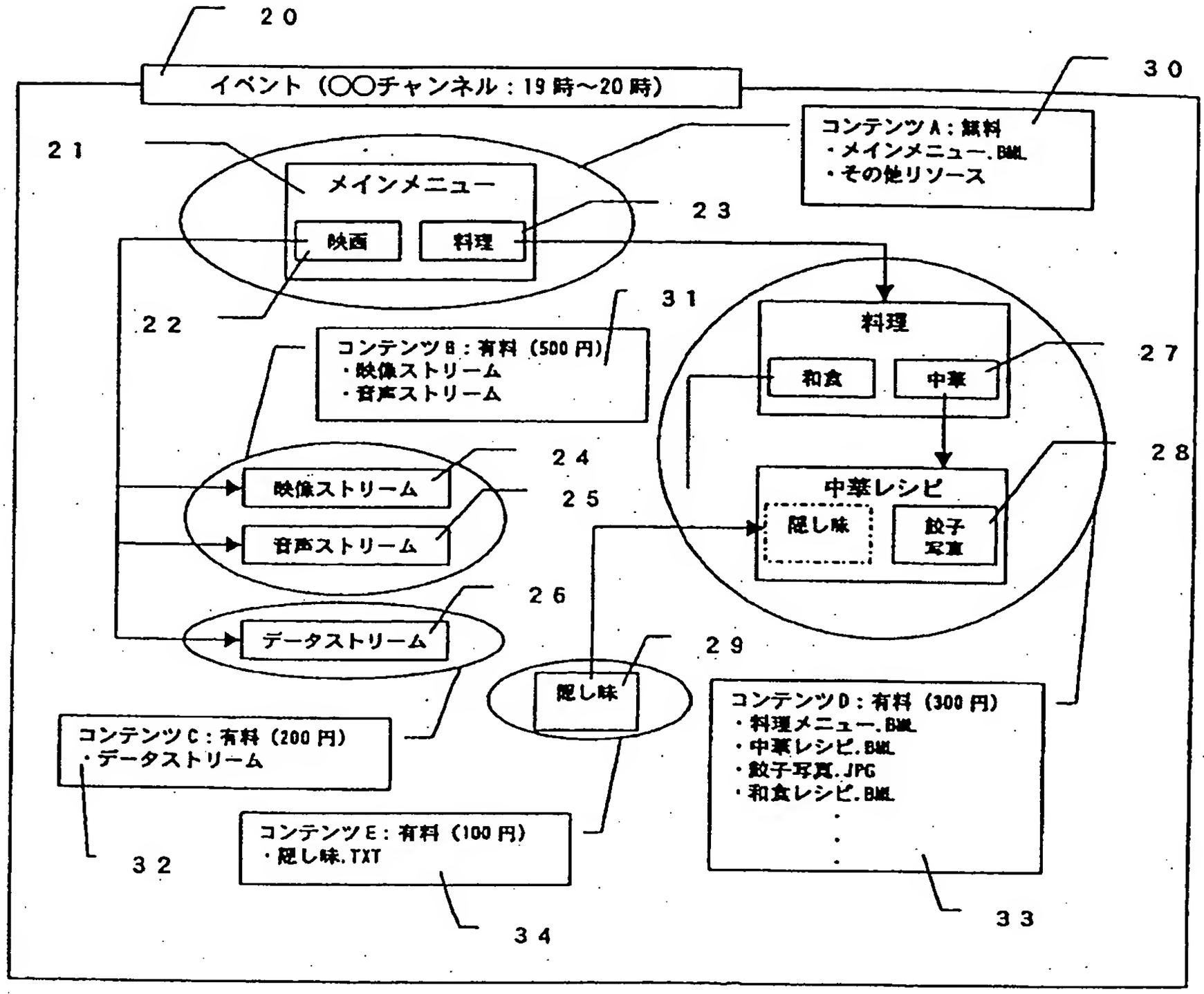
【図８】



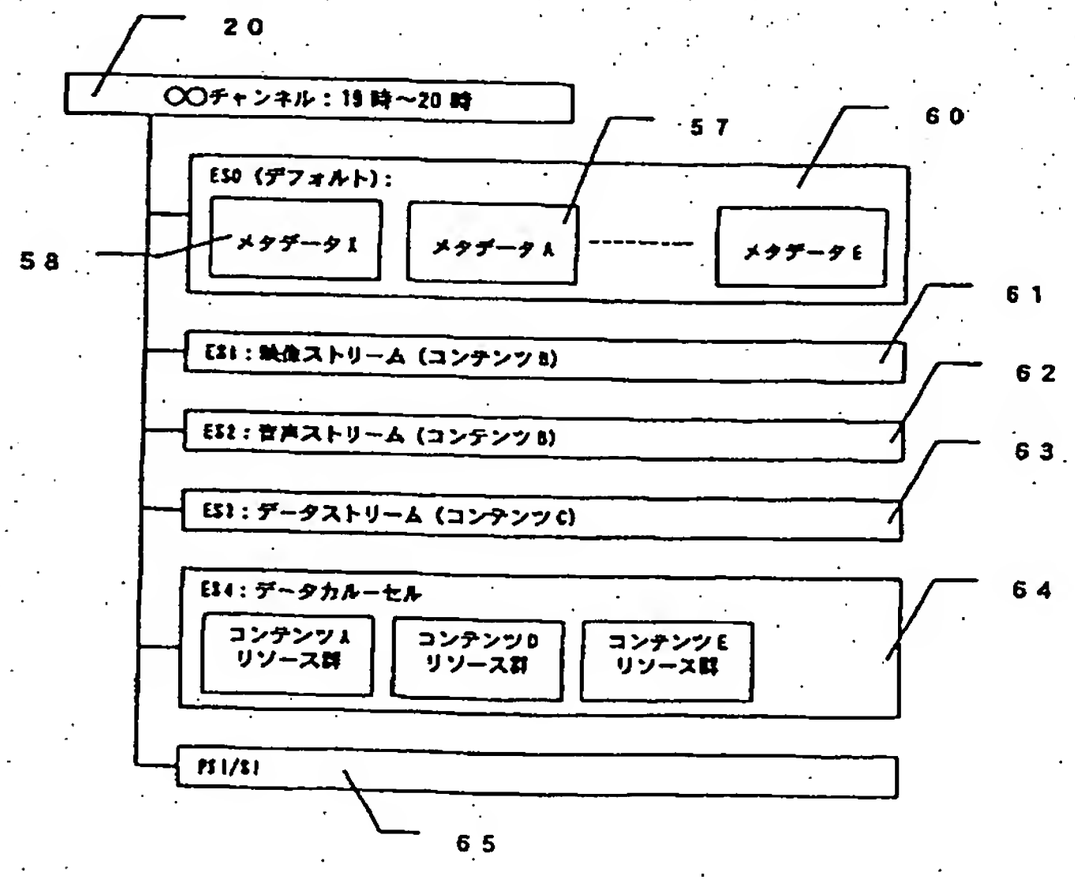
【図２２】



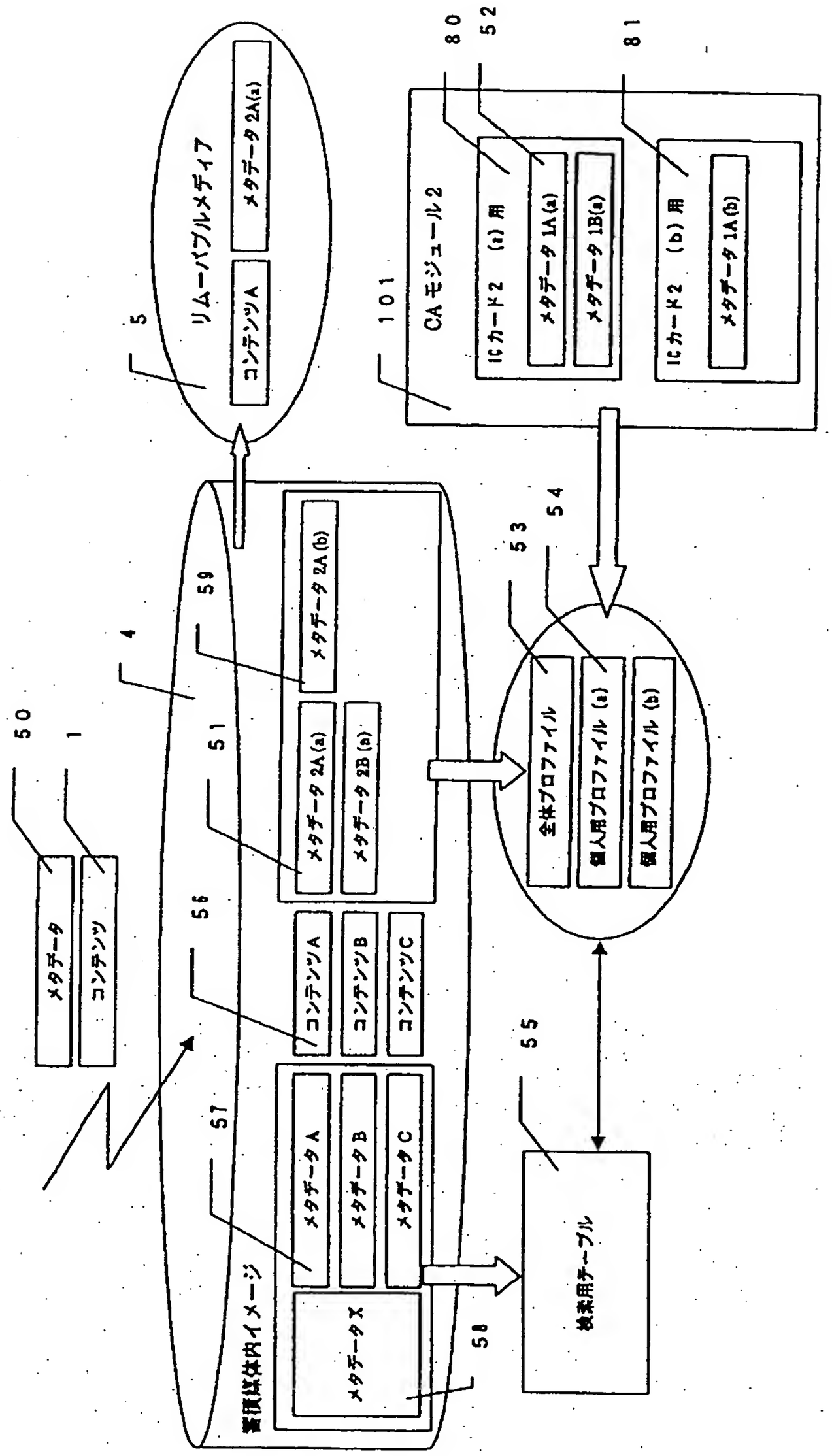
【図４】


20
イベント（○○チャンネル：19時～20時）
30
コンテンツA：無料
・メインメニュー.BML
・その他リソース
21
メインメニュー
映画
料理
23
22
31
コンテンツB：有料（500円）
・映像ストリーム
・音声ストリーム
料理
和食
中華
27
24
映像ストリーム
25
音声ストリーム
中華レシピ
隠し味
餃子写真
28
26
データストリーム
29
隠し味
コンテンツC：有料（200円）
・データストリーム
コンテンツD：有料（300円）
・料理メニュー.BML
・中華レシピ.BML
・餃子写真.JPG
・和食レシピ.BML
コンテンツE：有料（100円）
・隠し味.TXT
32
33
34

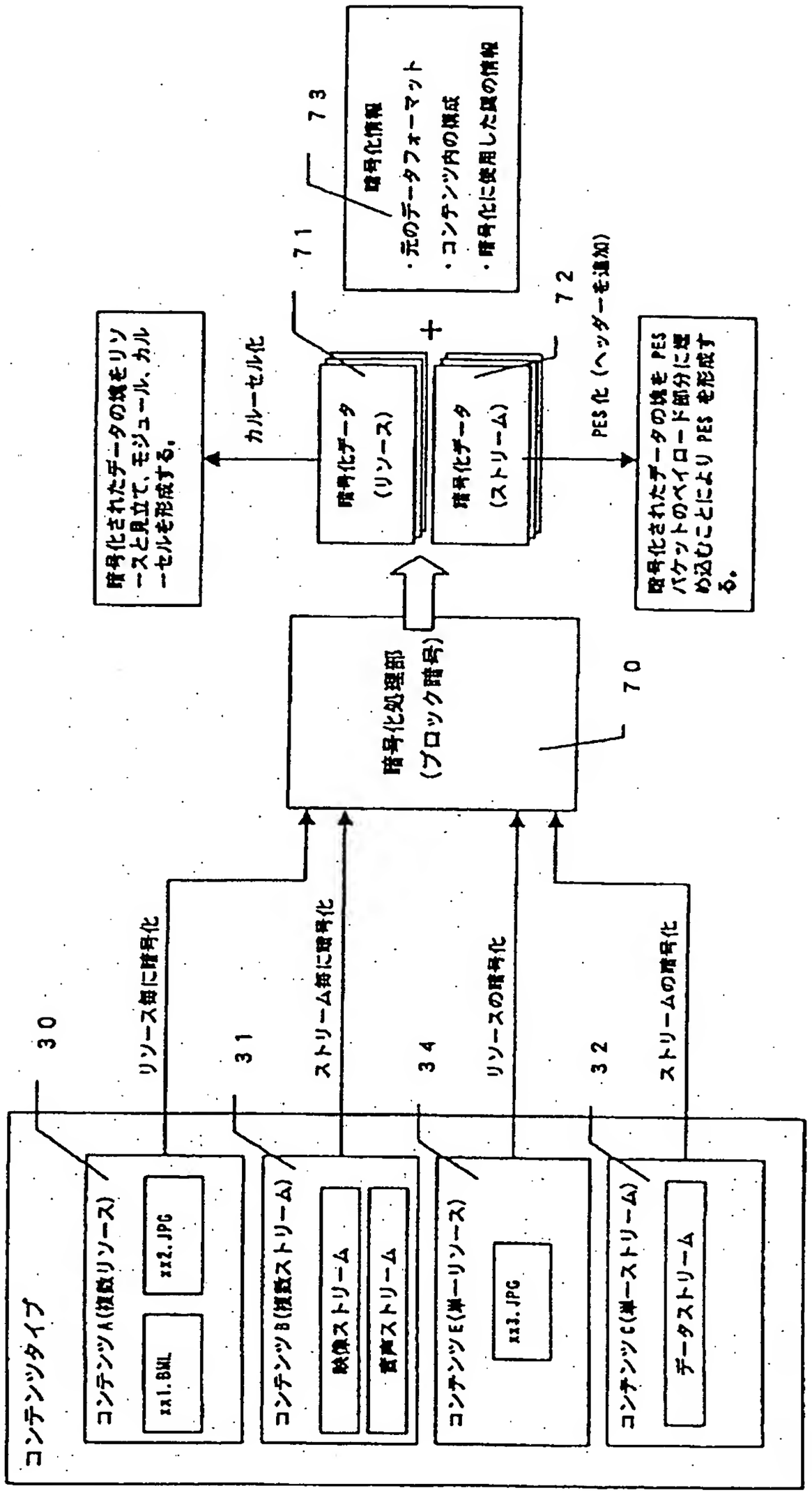
【図６】


20
○○チャンネル：19時～20時
57
60
ES0（デフォルト）：
メタデータA
メタデータB
メタデータE
58
61
ES1：映像ストリーム（コンテンツB）
62
ES2：音声ストリーム（コンテンツB）
63
ES3：データストリーム（コンテンツC）
64
ES4：データカルーセル
コンテンツA リソース群
コンテンツD リソース群
コンテンツE リソース群
PSI/SI
65

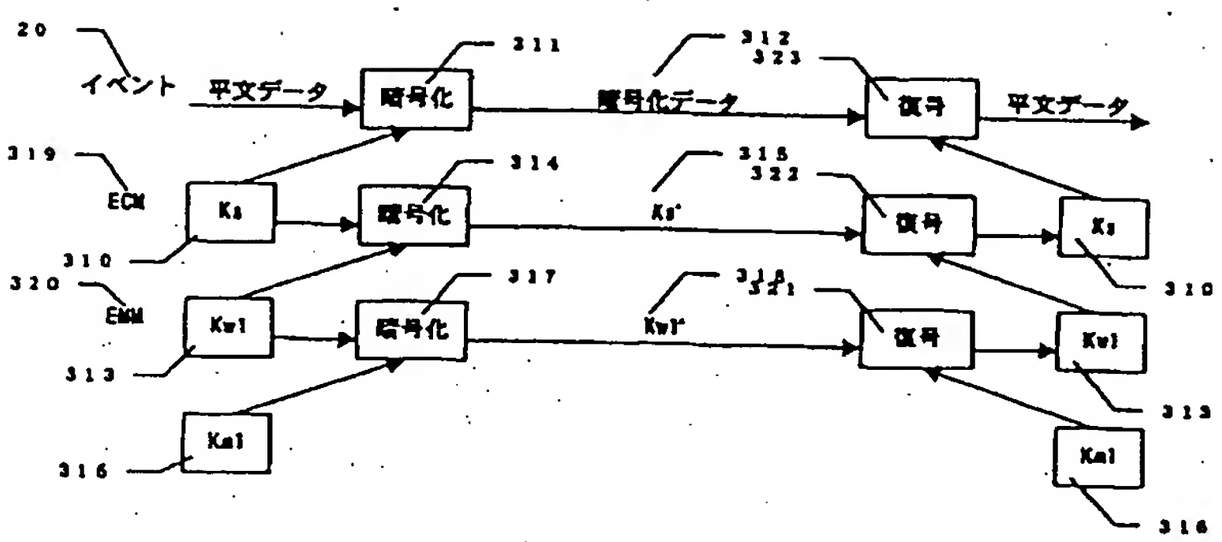
【図５】


80
52
81
101
CAモジュール2
ICカード2　(a)用
メタデータ1A(a)
メタデータ1B(a)
ICカード2　(b)用
メタデータ1A(b)
5
リムーバブルメディア
メタデータ2A(a)
コンテンツA
4
59
メタデータ2A(b)
メタデータ2A(a)
メタデータ2B(a)
50
1
メタデータ
コンテンツ
56
コンテンツA
コンテンツB
コンテンツC
57
メタデータA
メタデータB
メタデータC
メタデータX
58
蓄積媒体内イメージ
53
54
全体プロファイル
個人用プロファイル(a)
個人用プロファイル(b)
55
検索用テーブル

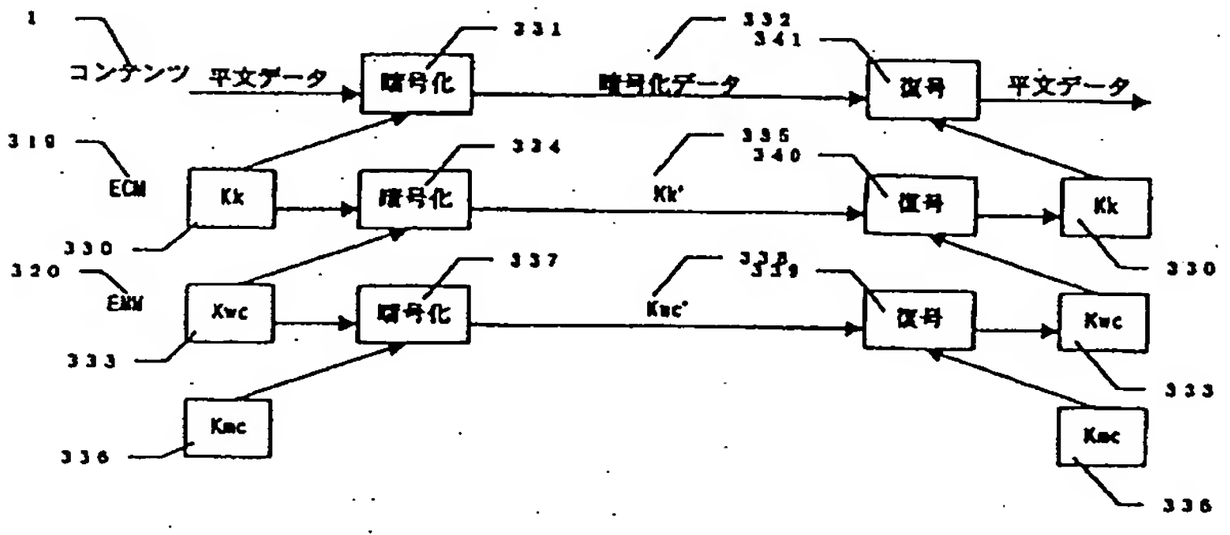
【図７】


コンテンツタイプ
コンテンツA(複数リソース)
xx1.BML
xx2.JPG
コンテンツB(複数ストリーム)
映像ストリーム
音声ストリーム
コンテンツE(単一リソース)
xx3.JPG
コンテンツC(単一ストリーム)
データストリーム
30
リソース毎に暗号化
31
ストリーム毎に暗号化
34
リソースの暗号化
32
ストリームの暗号化
暗号化処理部
(ブロック暗号)
70
暗号化データ
(リソース)
暗号化データ
(ストリーム)
カルーセル化
PES化 (ヘッダーも追加)
71
72
73
暗号化情報
・元のデータフォーマット
・コンテンツ内の構成
・暗号化に使用した鍵の情報
暗号化されたデータの塊をリソースと見立て、モジュール、カルーセルを形成する。
暗号化されたデータの塊を PES パケットのペイロード部分に埋め込むことにより PES を形成する。

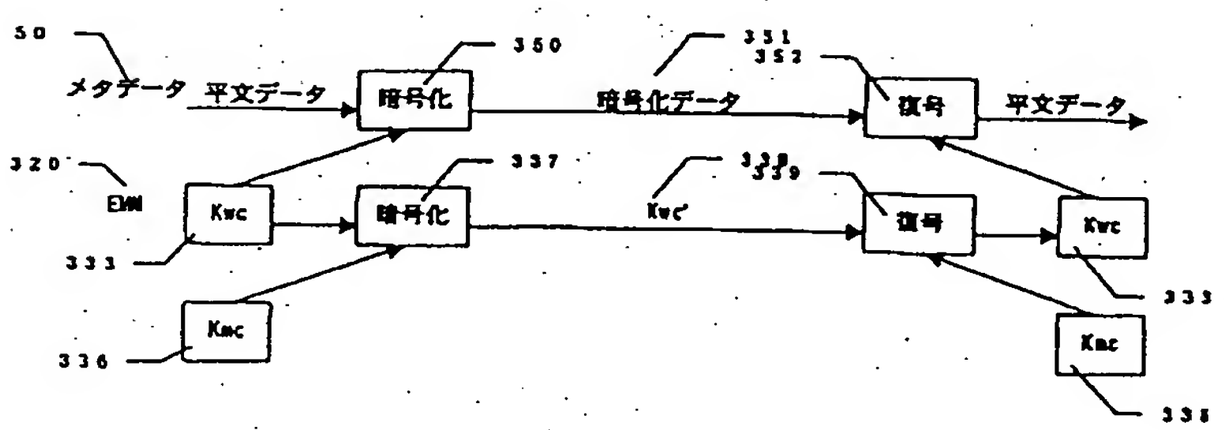
【図９】


20
イベント
平文データ
暗号化
311
暗号化データ
312
323
復号
平文データ
319
ECM
Ks
暗号化
314
Ks'
315
322
復号
Ks
310
320
EMM
Kwl
暗号化
317
Kwl'
318
321
復号
Kwl
313
Kml
316

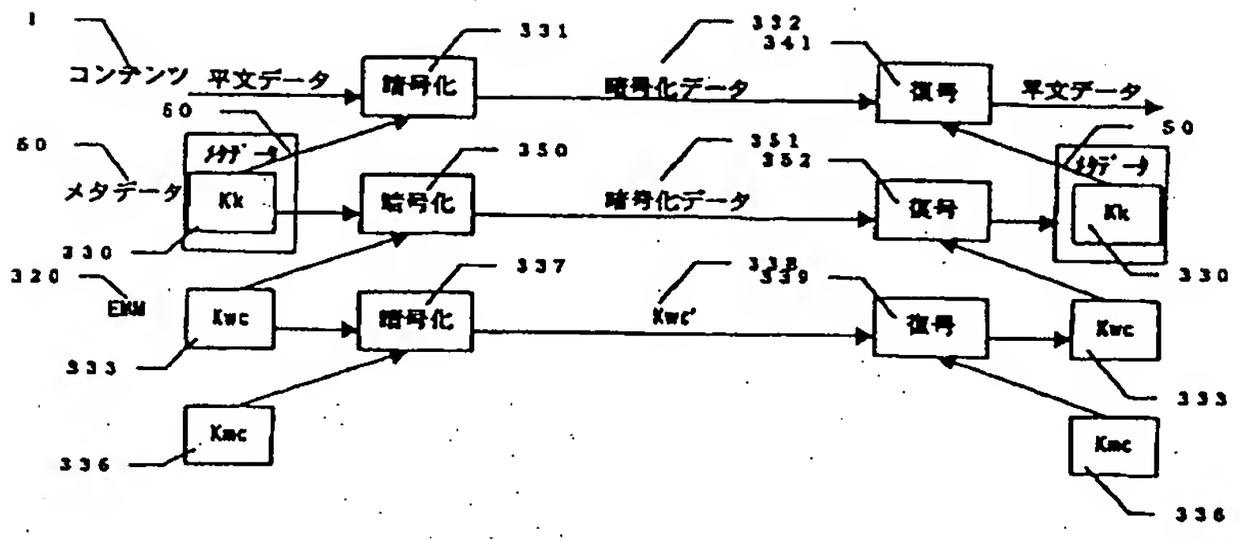
【図１０】


1
コンテンツ
平文データ
暗号化
331
暗号化データ
332
341
復号
平文データ
310
ECM
Kk
暗号化
334
Kk'
335
340
復号
Kk
330
320
EMM
Kwc
暗号化
337
Kwc'
338
339
復号
Kwc
333
Kmc
336

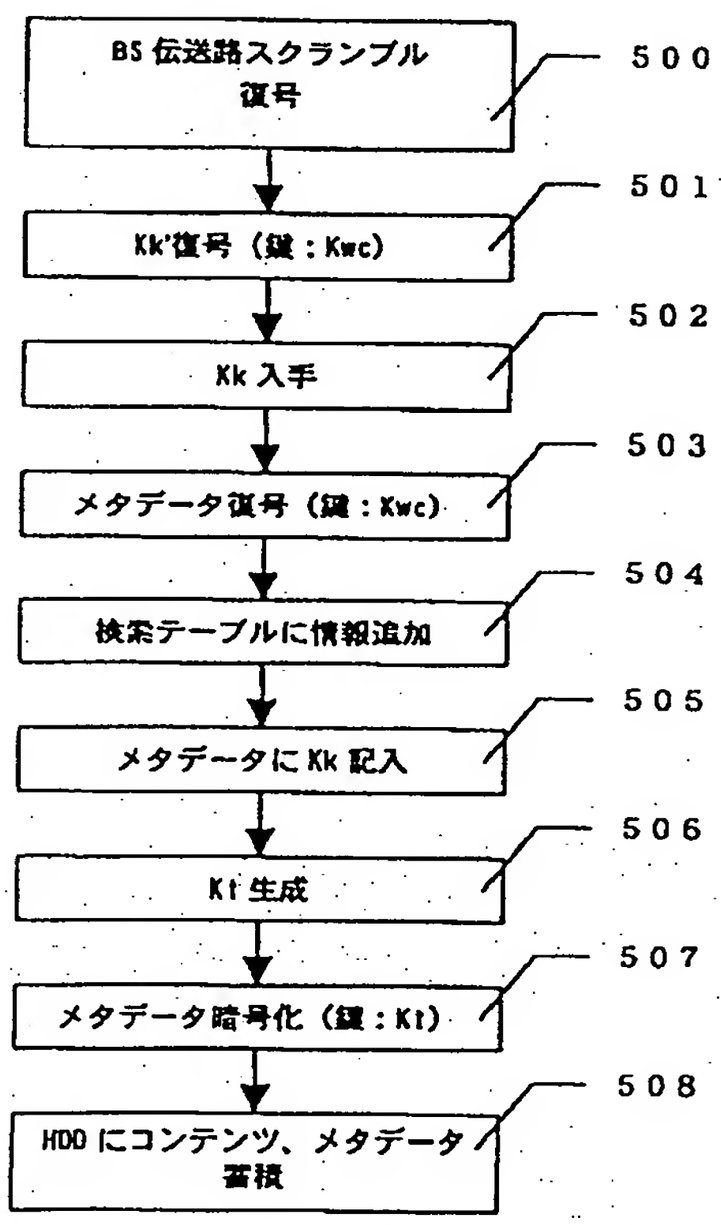
【図１１】


50
メタデータ
平文データ
暗号化
350
暗号化データ
351
352
復号
平文データ
320
EMM
Kwc
暗号化
337
Kwc'
338
339
復号
Kwc
333
Kmc
336

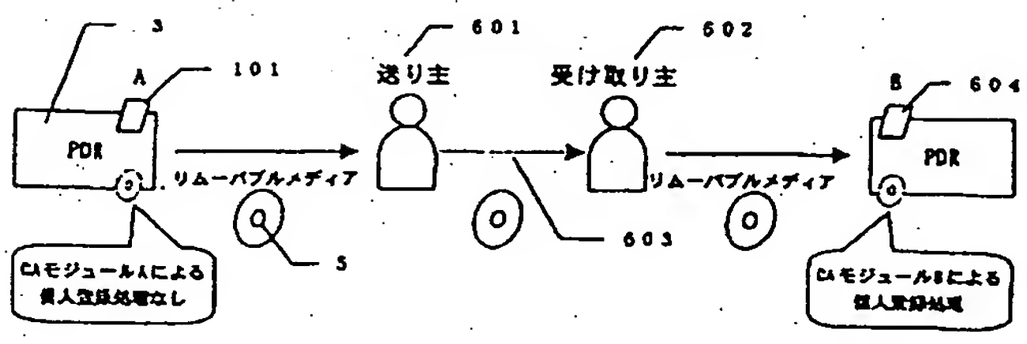
【図１２】


1
コンテンツ
平文データ
暗号化
331
332
341
暗号化データ
復号
平文データ
50
60
メタデータ
Kk
暗号化
350
351
352
暗号化データ
復号
Kk
330
320
EKM
Kwc
暗号化
337
338
339
Kwc'
復号
Kwc
333
Kmc
336
Kmc

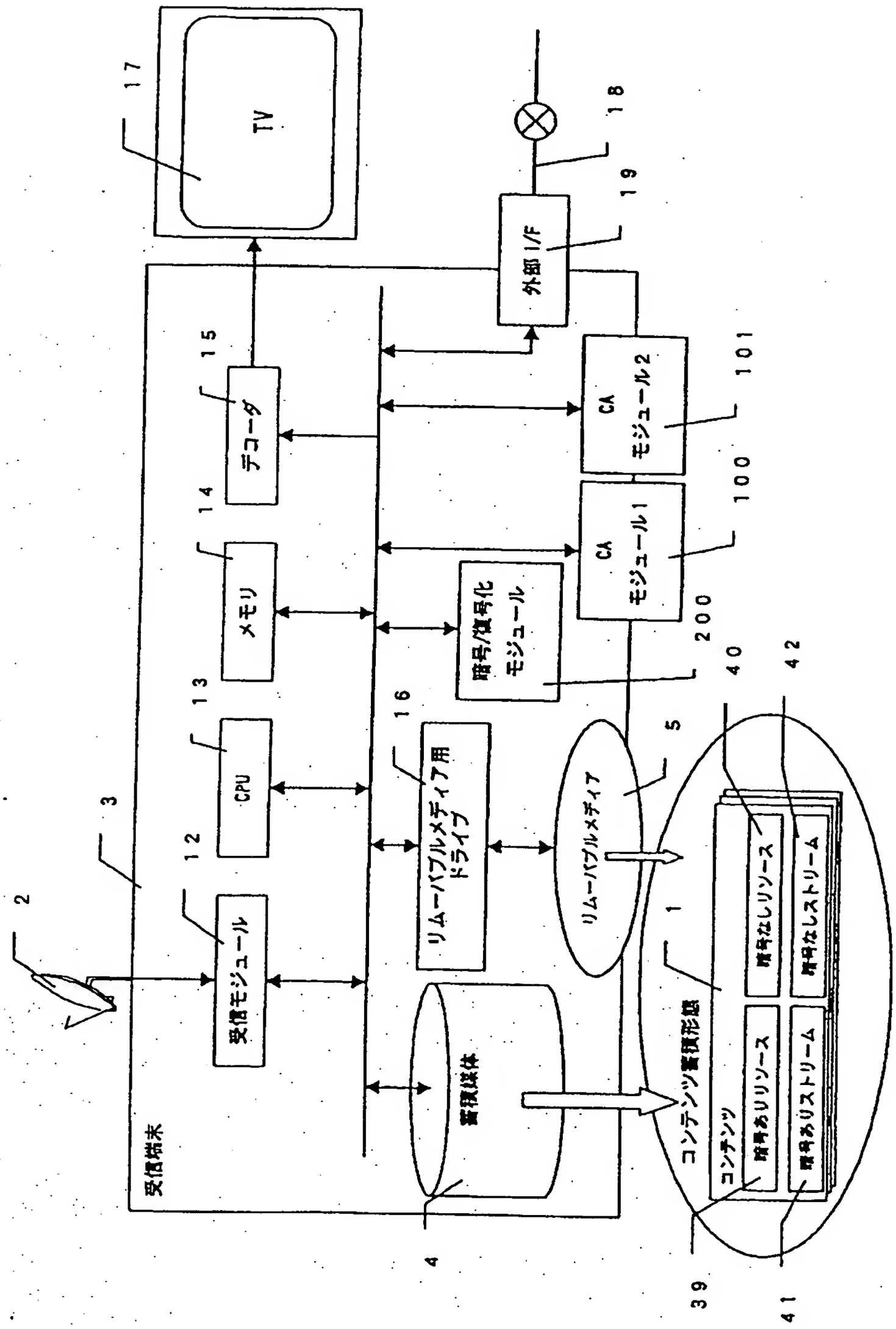
【図１６】


BS 伝送路スクランブル
復号
500
Kk'復号（鍵：Kwc）
501
Kk 入手
502
メタデータ復号（鍵：Kwc）
503
検索テーブルに情報追加
504
メタデータに Kk 記入
505
Kt 生成
506
メタデータ暗号化（鍵：Kt）
507
HDD にコンテンツ、メタデータ
蓄積
508

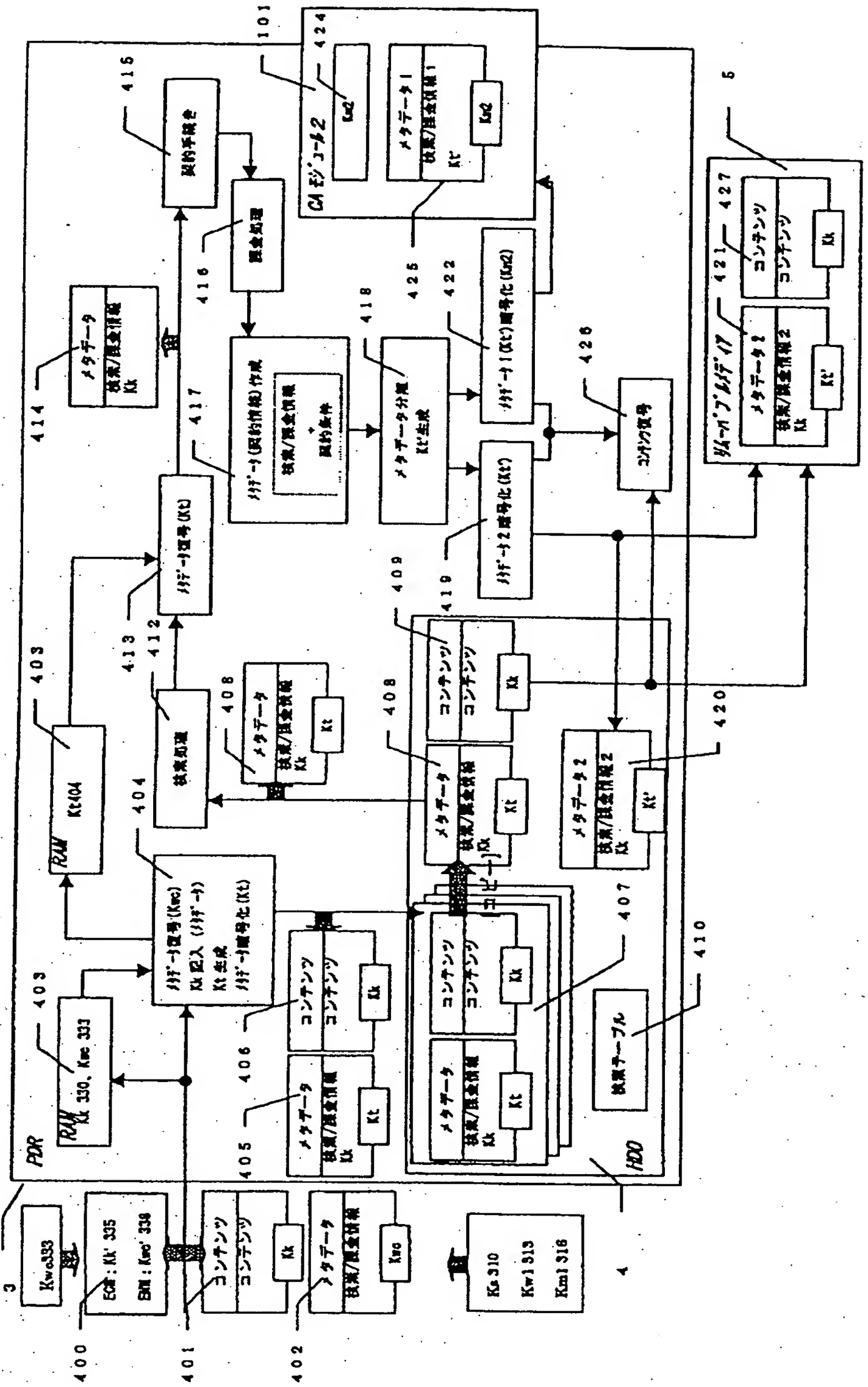
【図２１】


3
A
101
PDR
リムーバブルメディア
5
CAモジュールAによる
個人登録処理なし
601
送り主
602
受け取り主
603
リムーバブルメディア
B
604
PDR
CAモジュールBによる
個人登録処理

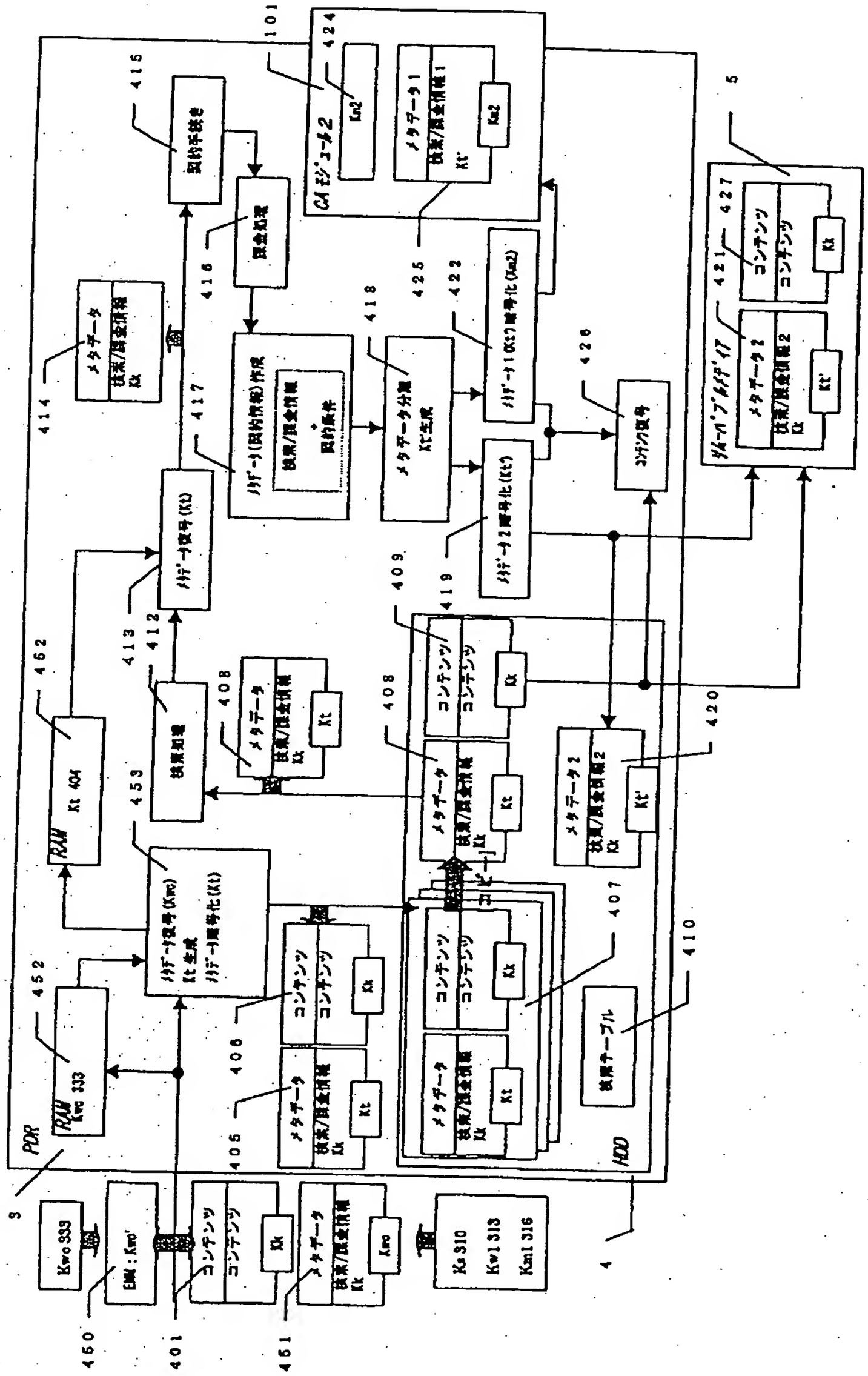
【図１３】


受信端末
2
3
4
TV
17
18
19
外部I/F
15
デコーダ
14
メモリ
13
CPU
12
受信モジュール
16
リムーバブルメディア用ドライブ
蓄積媒体
5
リムーバブルメディア
CA モジュール2
101
CA モジュール1
100
暗号/復号化モジュール
200
40
42
1
暗号なしリソース
暗号なしストリーム
コンテンツ蓄積形態
コンテンツ
暗号ありリソース
暗号ありストリーム
39
41

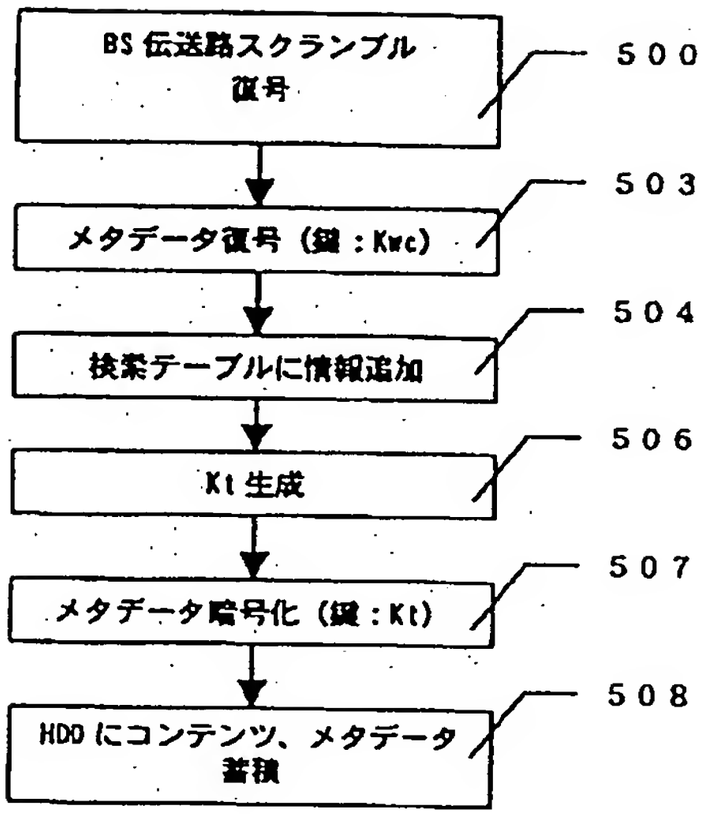
【図１４】


101
424
415
契約手続き
課金処理
416
メタデータ1
技術/属性情報1
Kt'
Kt2
CM モジュール2
5
427
コンテンツ
Kk
421
メタデータ2
技術/属性情報2
Kt'
ルールブルモデル
425
422
418
コンテンツ1(Kt)暗号化
426
コンテンツ暗号
メタデータ分離
Kt'生成
417
コンテンツ1(契約情報)作成
技術/属性情報
契約条件
414
メタデータ
技術/属性情報
Kk
413
コンテンツ1暗号(Kt)
412
403
Kt404
RAM
404
技術処理
408
メタデータ
技術/属性情報
Kk
409
410
コンテンツ2暗号化(Kt)
コンテンツ
メタデータ
技術/属性情報
Kk
Kt'
420
メタデータ2
技術/属性情報2
Kt'
コンテンツ1暗号(Kmc)
Kk記入(コンテンツ)
Kt生成
コンテンツ暗号化(Kt)
407
410
406
405
PDR
RAM
Kt 330, Kwc 333
Kwc333
EGM : Kk' 335
BMM : Kwc' 338
400
401
402
Kc 310
Kwl 313
Kml 316
HDD
4

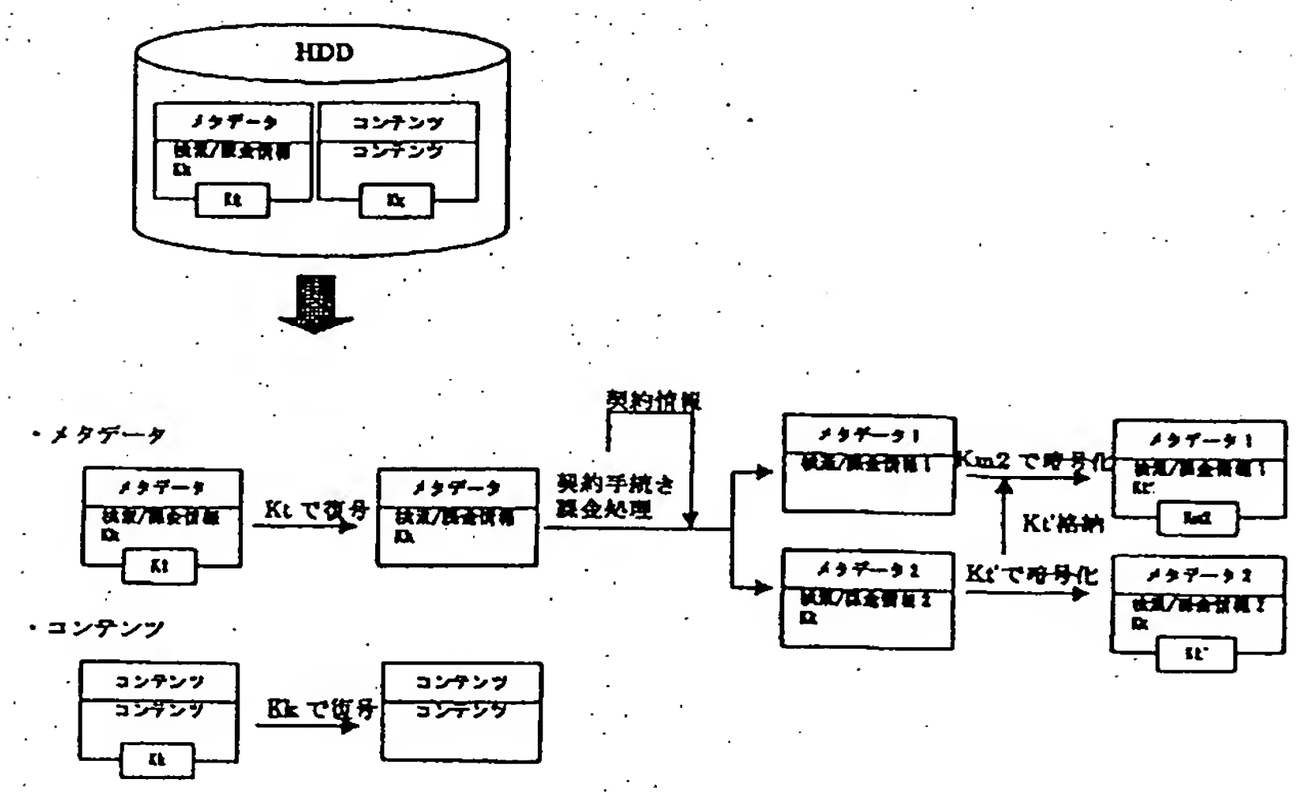
【図１５】


101
424
415
416
425
422
418
417
426
427
421
5
420
414
413
412
408
409
419
462
453
407
410
452
106
105
403
402
404
333
339
313
316
310
460
401
461
3
4
PDR
RAM
HDD
EMI
メタデータ
コンテンツ
Kt
Kt'
Kt2
Kt2'
Kt3
Kt4
Kt5
Kt6
Kt7
Kt8
Kt9
Kt10
Kt11
Kt12
Kt13
Kt14
Kt15
Kt16
Kt17
Kt18
Kt19
Kt20
Kt21
Kt22
Kt23
Kt24
Kt25
Kt26
Kt27
Kt28
Kt29
Kt30
Kt31
Kt32
Kt33
Kt34
Kt35
Kt36
Kt37
Kt38
Kt39
Kt40
Kt41
Kt42
Kt43
Kt44
Kt45
Kt46
Kt47
Kt48
Kt49
Kt50
Kt51
Kt52
Kt53
Kt54
Kt55
Kt56
Kt57
Kt58
Kt59
Kt60
Kt61
Kt62
Kt63
Kt64
Kt65
Kt66
Kt67
Kt68
Kt69
Kt70
Kt71
Kt72
Kt73
Kt74
Kt75
Kt76
Kt77
Kt78
Kt79
Kt80
Kt81
Kt82
Kt83
Kt84
Kt85
Kt86
Kt87
Kt88
Kt89
Kt90
Kt91
Kt92
Kt93
Kt94
Kt95
Kt96
Kt97
Kt98
Kt99
Kt100
Kt101
Kt102
Kt103
Kt104
Kt105
Kt106
Kt107
Kt108
Kt109
Kt110
Kt111
Kt112
Kt113
Kt114
Kt115
Kt116
Kt117
Kt118
Kt119
Kt120
Kt121
Kt122
Kt123
Kt124
Kt125
Kt126
Kt127
Kt128
Kt129
Kt130
Kt131
Kt132
Kt133
Kt134
Kt135
Kt136
Kt137
Kt138
Kt139
Kt140
Kt141
Kt142
Kt143
Kt144
Kt145
Kt146
Kt147
Kt148
Kt149
Kt150
Kt151
Kt152
Kt153
Kt154
Kt155
Kt156
Kt157
Kt158
Kt159
Kt160
Kt161
Kt162
Kt163
Kt164
Kt165
Kt166
Kt167
Kt168
Kt169
Kt170
Kt171
Kt172
Kt173
Kt174
Kt175
Kt176
Kt177
Kt178
Kt179
Kt180
Kt181
Kt182
Kt183
Kt184
Kt185
Kt186
Kt187
Kt188
Kt189
Kt190
Kt191
Kt192
Kt193
Kt194
Kt195
Kt196
Kt197
Kt198
Kt199
Kt200
Kt201
Kt202
Kt203
Kt204
Kt205
Kt206
Kt207
Kt208
Kt209
Kt210
Kt211
Kt212
Kt213
Kt214
Kt215
Kt216
Kt217
Kt218
Kt219
Kt220
Kt221
Kt222
Kt223
Kt224
Kt225
Kt226
Kt227
Kt228
Kt229
Kt230
Kt231
Kt232
Kt233
Kt234
Kt235
Kt236
Kt237
Kt238
Kt239
Kt240
Kt241
Kt242
Kt243
Kt244
Kt245
Kt246
Kt247
Kt248
Kt249
Kt250
Kt251
Kt252
Kt253
Kt254
Kt255
Kt256
Kt257
Kt258
Kt259
Kt260
Kt261
Kt262
Kt263
Kt264
Kt265
Kt266
Kt267
Kt268
Kt269
Kt270
Kt271
Kt272
Kt273
Kt274
Kt275
Kt276
Kt277
Kt278
Kt279
Kt280
Kt281
Kt282
Kt283
Kt284
Kt285
Kt286
Kt287
Kt288
Kt289
Kt290
Kt291
Kt292
Kt293
Kt294
Kt295
Kt296
Kt297
Kt298
Kt299
Kt300
Kt301
Kt302
Kt303
Kt304
Kt305
Kt306
Kt307
Kt308
Kt309
Kt310
Kt311
Kt312
Kt313
Kt314
Kt315
Kt316
Kt317
Kt318
Kt319
Kt320
Kt321
Kt322
Kt323
Kt324
Kt325
Kt326
Kt327
Kt328
Kt329
Kt330
Kt331
Kt332
Kt333
Kt334
Kt335
Kt336
Kt337
Kt338
Kt339
Kt340
Kt341
Kt342
Kt343
Kt344
Kt345
Kt346
Kt347
Kt348
Kt349
Kt350
Kt351
Kt352
Kt353
Kt354
Kt355
Kt356
Kt357
Kt358
Kt359
Kt360
Kt361
Kt362
Kt363
Kt364
Kt365
Kt366
Kt367
Kt368
Kt369
Kt370
Kt371
Kt372
Kt373
Kt374
Kt375
Kt376
Kt377
Kt378
Kt379
Kt380
Kt381
Kt382
Kt383
Kt384
Kt385
Kt386
Kt387
Kt388
Kt389
Kt390
Kt391
Kt392
Kt393
Kt394
Kt395
Kt396
Kt397
Kt398
Kt399
Kt400
Kt401
Kt402
Kt403
Kt404
Kt405
Kt406
Kt407
Kt408
Kt409
Kt410
Kt411
Kt412
Kt413
Kt414
Kt415
Kt416
Kt417
Kt418
Kt419
Kt420
Kt421
Kt422
Kt423
Kt424
Kt425
Kt426
Kt427
Kt428
Kt429
Kt430
Kt431
Kt432
Kt433
Kt434
Kt435
Kt436
Kt437
Kt438
Kt439
Kt440
Kt441
Kt442
Kt443
Kt444
Kt445
Kt446
Kt447
Kt448
Kt449
Kt450
Kt451
Kt452
Kt453
Kt454
Kt455
Kt456
Kt457
Kt458
Kt459
Kt460
Kt461
Kt462
Kt463
Kt464
Kt465
Kt466
Kt467
Kt468
Kt469
Kt470
Kt471
Kt472
Kt473
Kt474
Kt475
Kt476
Kt477
Kt478
Kt479
Kt480
Kt481
Kt482
Kt483
Kt484
Kt485
Kt486
Kt487
Kt488
Kt489
Kt490
Kt491
Kt492
Kt493
Kt494
Kt495
Kt496
Kt497
Kt498
Kt499
Kt500
Kt501
Kt502
Kt503
Kt504
Kt505
Kt506
Kt507
Kt508
Kt509
Kt510
Kt511
Kt512
Kt513
Kt514
Kt515
Kt516
Kt517
Kt518
Kt519
Kt520
Kt521
Kt522
Kt523
Kt524
Kt525
Kt526
Kt527
Kt528
Kt529
Kt530
Kt531
Kt532
Kt533
Kt534
Kt535
Kt536
Kt537
Kt538
Kt539
Kt540
Kt541
Kt542
Kt543
Kt544
Kt545
Kt546
Kt547
Kt548
Kt549
Kt550
Kt551
Kt552
Kt553
Kt554
Kt555
Kt556
Kt557
Kt558
Kt559
Kt560
Kt561
Kt562
Kt563
Kt564
Kt565
Kt566
Kt567
Kt568
Kt569
Kt570
Kt571
Kt572
Kt573
Kt574
Kt575
Kt576
Kt577
Kt578
Kt579
Kt580
Kt581
Kt582
Kt583
Kt584
Kt585
Kt586
Kt587
Kt588
Kt589
Kt590
Kt591
Kt592
Kt593
Kt594
Kt595
Kt596
Kt597
Kt598
Kt599
Kt600
Kt601
Kt602
Kt603
Kt604
Kt605
Kt606
Kt607
Kt608
Kt609
Kt610
Kt611
Kt612
Kt613
Kt614
Kt615
Kt616
Kt617
Kt618
Kt619
Kt620
Kt621
Kt622
Kt623
Kt624
Kt625
Kt626
Kt627
Kt628
Kt629
Kt630
Kt631
Kt632
Kt633
Kt634
Kt635
Kt636
Kt637
Kt638
Kt639
Kt640
Kt641
Kt642
Kt643
Kt644
Kt645
Kt646
Kt647
Kt648
Kt649
Kt650
Kt651
Kt652
Kt653
Kt654
Kt655
Kt656
Kt657
Kt658
Kt659
Kt660
Kt661
Kt662
Kt663
Kt664
Kt665
Kt666
Kt667
Kt668
Kt669
Kt670
Kt671
Kt672
Kt673
Kt674
Kt675
Kt676
Kt677
Kt678
Kt679
Kt680
Kt681
Kt682
Kt683
Kt684
Kt685
Kt686
Kt687
Kt688
Kt689
Kt690
Kt691
Kt692
Kt693
Kt694
Kt695
Kt696
Kt697
Kt698
Kt699
Kt700
Kt701
Kt702
Kt703
Kt704
Kt705
Kt706
Kt707
Kt708
Kt709
Kt710
Kt711
Kt712
Kt713
Kt714
Kt715
Kt716
Kt717
Kt718
Kt719
Kt720
Kt721
Kt722
Kt723
Kt724
Kt725
Kt726
Kt727
Kt728
Kt729
Kt730
Kt731
Kt732
Kt733
Kt734
Kt735
Kt736
Kt737
Kt738
Kt739
Kt740
Kt741
Kt742
Kt743
Kt744
Kt745
Kt746
Kt747
Kt748
Kt749
Kt750
Kt751
Kt752
Kt753
Kt754
Kt755
Kt756
Kt757
Kt758
Kt759
Kt760
Kt761
Kt762
Kt763
Kt764
Kt765
Kt766
Kt767
Kt768
Kt769
Kt770
Kt771
Kt772
Kt773
Kt774
Kt775
Kt776
Kt777
Kt778
Kt779
Kt780
Kt781
Kt782
Kt783
Kt784
Kt785
Kt786
Kt787
Kt788
Kt789
Kt790
Kt791
Kt792
Kt793
Kt794
Kt795
Kt796
Kt797
Kt798
Kt799
Kt800
Kt801
Kt802
Kt803
Kt804
Kt805
Kt806
Kt807
Kt808
Kt809
Kt810
Kt811
Kt812
Kt813
Kt814
Kt815
Kt816
Kt817
Kt818
Kt819
Kt820
Kt821
Kt822
Kt823
Kt824
Kt825
Kt826
Kt827
Kt828
Kt829
Kt830
Kt831
Kt832
Kt833
Kt834
Kt835
Kt836
Kt837
Kt838
Kt839
Kt840
Kt841
Kt842
Kt843
Kt844
Kt845
Kt846
Kt847
Kt848
Kt849
Kt850
Kt851
Kt852
Kt853
Kt854
Kt855
Kt856
Kt857
Kt858
Kt859
Kt860
Kt861
Kt862
Kt863
Kt864
Kt865
Kt866
Kt867
Kt868
Kt869
Kt870
Kt871
Kt872
Kt873
Kt874
Kt875
Kt876
Kt877
Kt878
Kt879
Kt880
Kt881
Kt882
Kt883
Kt884
Kt885
Kt886
Kt887
Kt888
Kt889
Kt890
Kt891
Kt892
Kt893
Kt894
Kt895
Kt896
Kt897
Kt898
Kt899
Kt900
Kt901
Kt902
Kt903
Kt904
Kt905
Kt906
Kt907
Kt908
Kt909
Kt910
Kt911
Kt912
Kt913
Kt914
Kt915
Kt916
Kt917
Kt918
Kt919
Kt920
Kt921
Kt922
Kt923
Kt924
Kt925
Kt926
Kt927
Kt928
Kt929
Kt930
Kt931
Kt932
Kt933
Kt934
Kt935
Kt936
Kt937
Kt938
Kt939
Kt940
Kt941
Kt942
Kt943
Kt944
Kt945
Kt946
Kt947
Kt948
Kt949
Kt950
Kt951
Kt952
Kt953
Kt954
Kt955
Kt956
Kt957
Kt958
Kt959
Kt960
Kt961
Kt962
Kt963
Kt964
Kt965
Kt966
Kt967
Kt968
Kt969
Kt970
Kt971
Kt972
Kt973
Kt974
Kt975
Kt976
Kt977
Kt978
Kt979
Kt980
Kt981
Kt982
Kt983
Kt984
Kt985
Kt986
Kt987
Kt988
Kt989
Kt990
Kt991
Kt992
Kt993
Kt994
Kt995
Kt996
Kt997
Kt998
Kt999
Kt1000

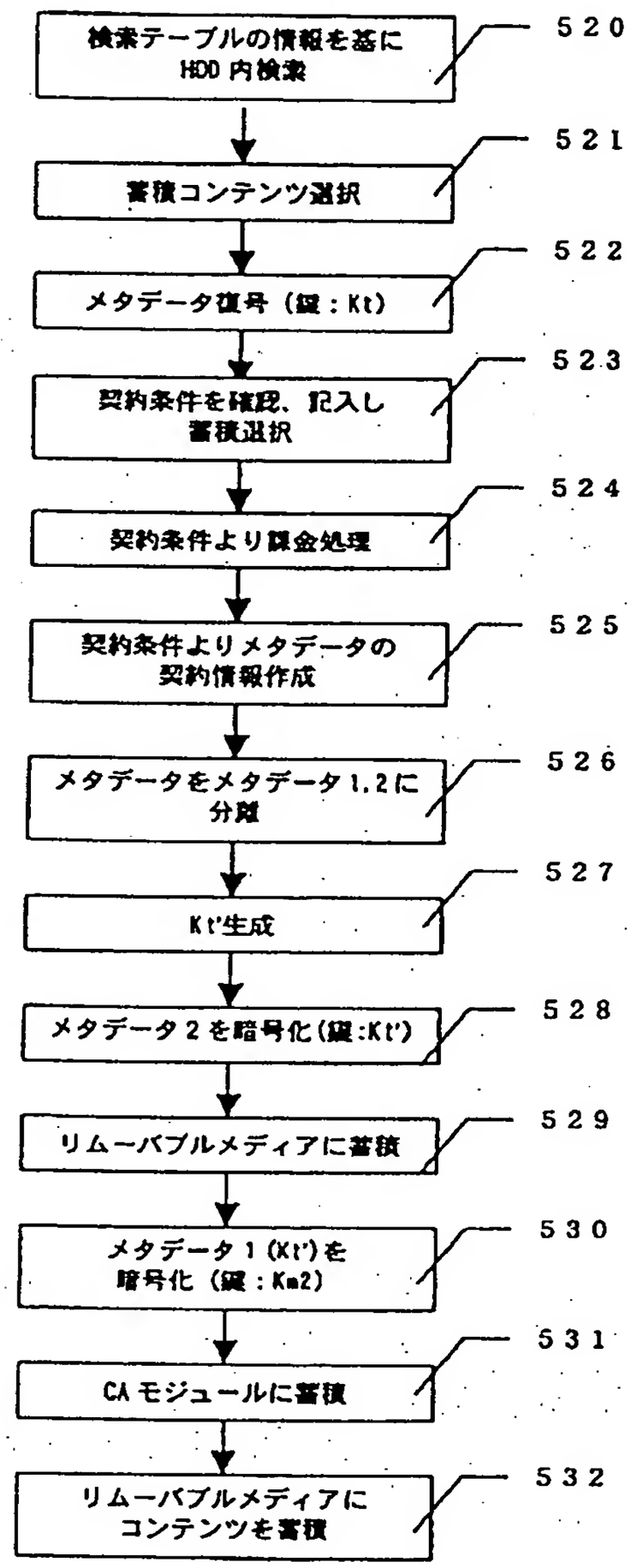
【図１７】


BS 伝送路スクランブル
復号
500
メタデータ復号（鍵：Kwc）
503
検索テーブルに情報追加
504
Kt 生成
506
メタデータ暗号化（鍵：Kt）
507
HDD にコンテンツ、メタデータ
蓄積
508

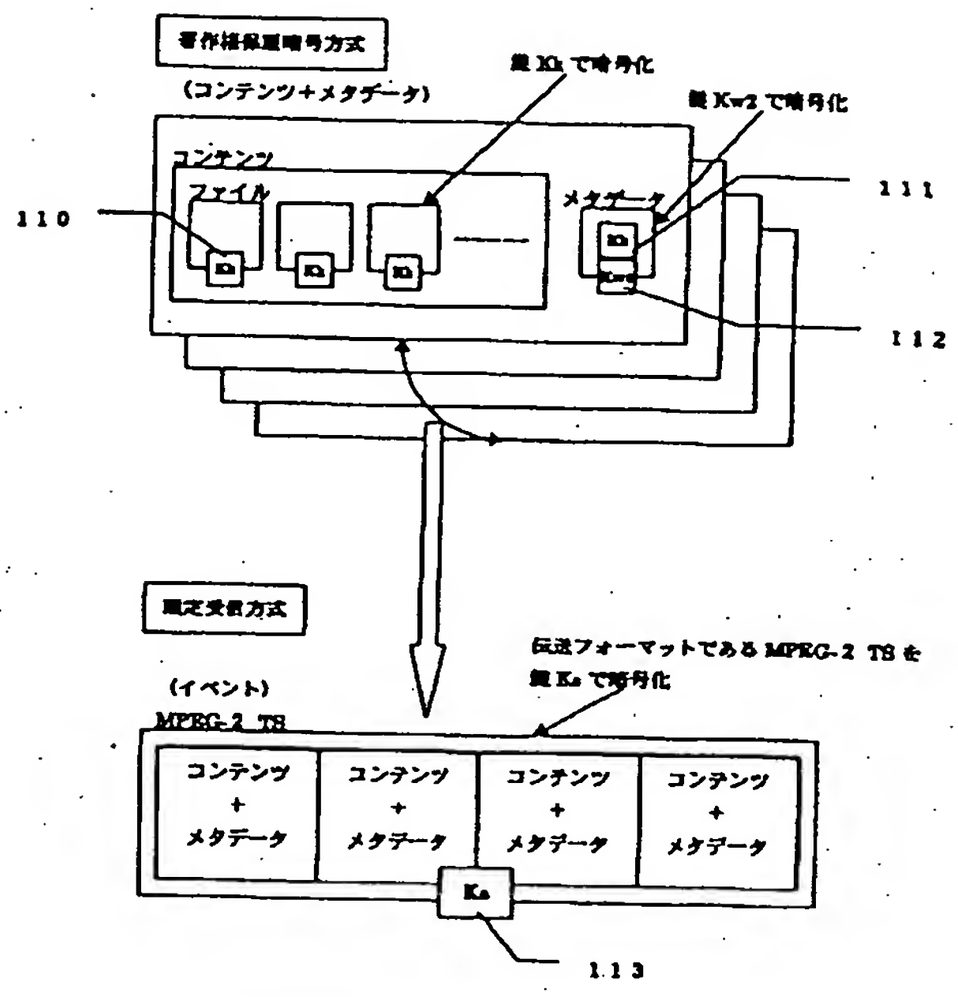
【図２４】


HDD
メタデータ
コンテンツ
Kt
Kc
・メタデータ
Kt で復号
契約情報
契約手続き
課金処理
Km2 で暗号化
Kt'格納
Kt'で暗号化
・コンテンツ
Kc で復号

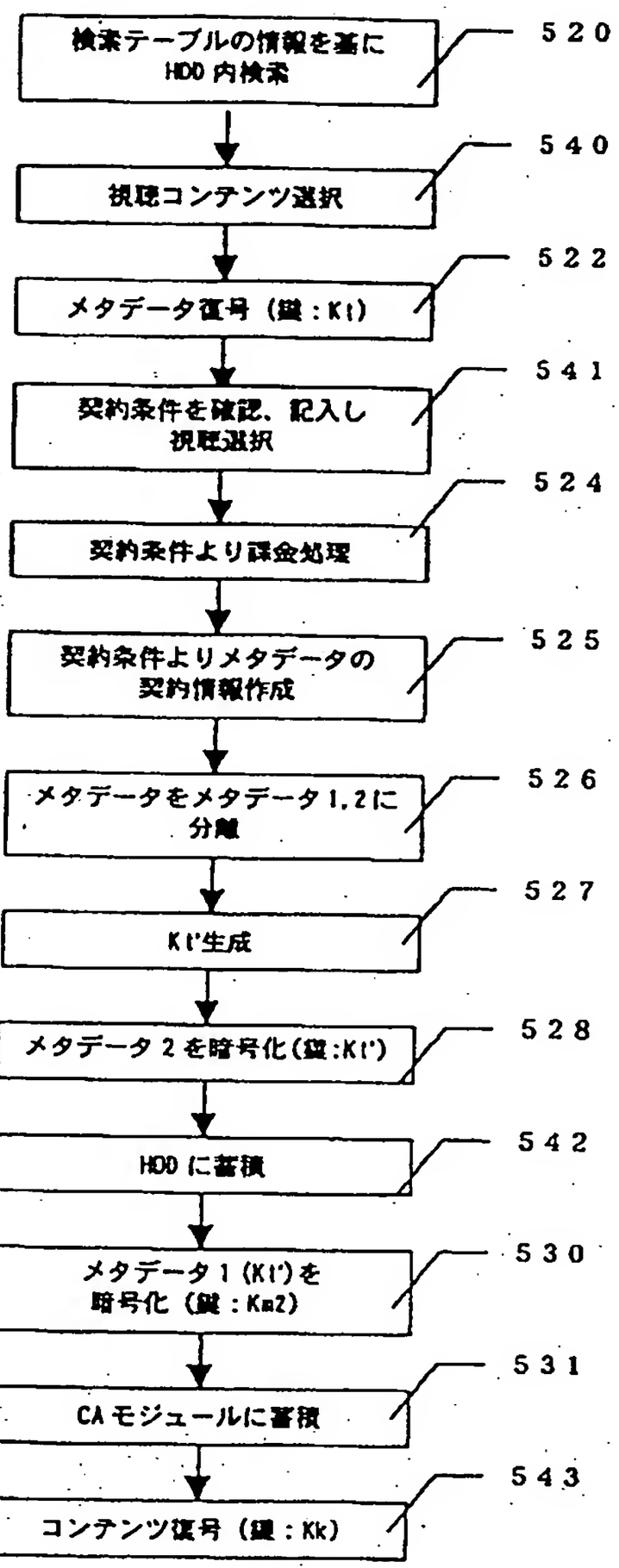
【図１８】


検索テーブルの情報を基に HDD 内検索
520
蓄積コンテンツ選択
521
メタデータ復号（鍵：Kt）
522
契約条件を確認、記入し 蓄積選択
523
契約条件より課金処理
524
契約条件よりメタデータの 契約情報作成
525
メタデータをメタデータ 1,2 に 分離
526
Kt'生成
527
メタデータ 2 を暗号化（鍵:Kt'）
528
リムーバブルメディアに蓄積
529
メタデータ 1（Kt'）を 暗号化（鍵：Km2）
530
CA モジュールに蓄積
531
リムーバブルメディアに コンテンツを蓄積
532

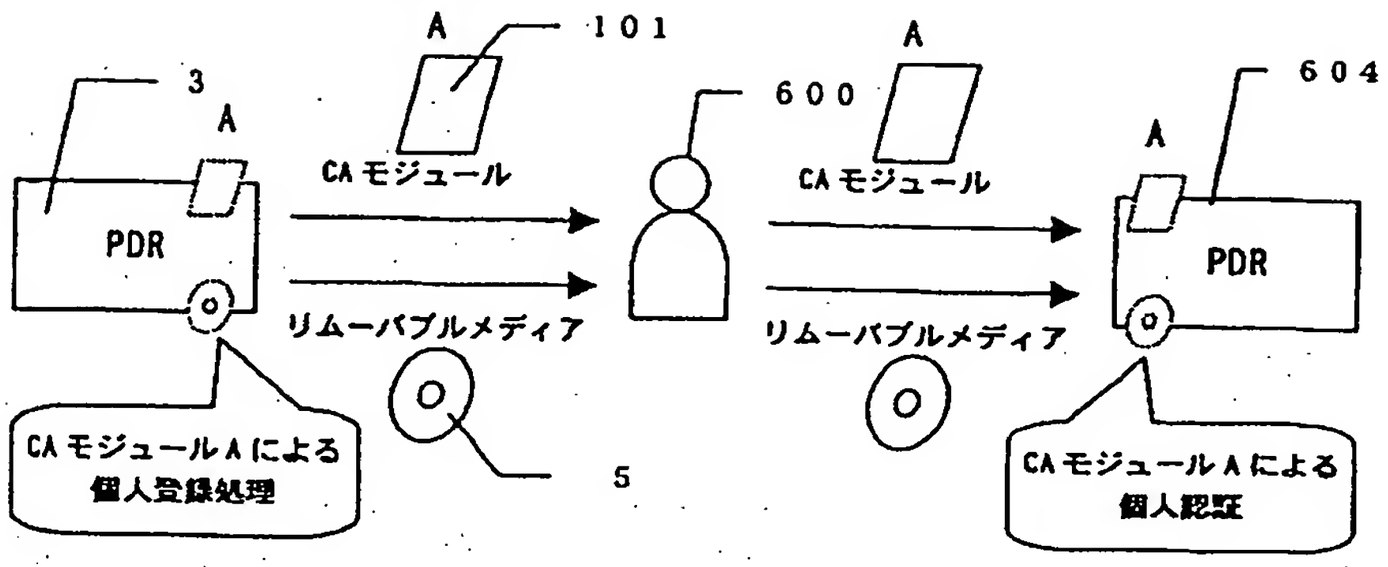
【図２３】


著作権保護暗号方式
(コンテンツ+メタデータ)
鍵 Kt で暗号化
鍵 Km2 で暗号化
コンテンツ ファイル
メタデータ
110
111
112
限定受信方式
伝送フォーマットである MPEG-2 TS を 鍵 Ks で暗号化
(イベント) MPEG-2 TS
コンテンツ + メタデータ
コンテンツ + メタデータ
コンテンツ + メタデータ
コンテンツ + メタデータ
Ks
113

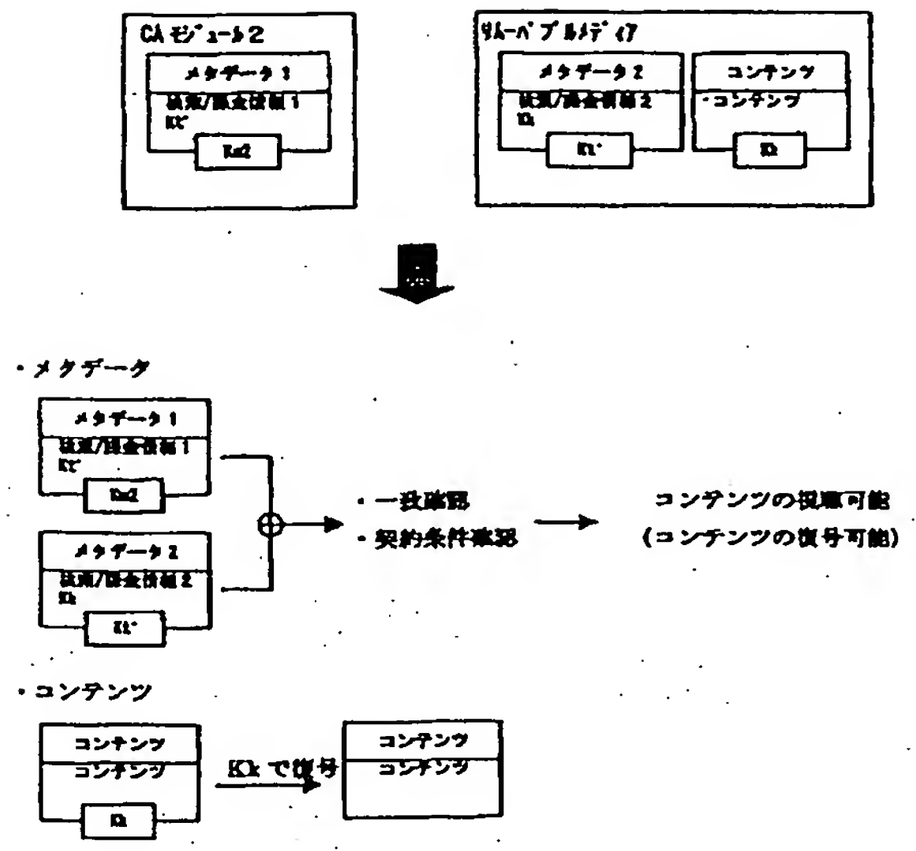
【図１９】


検索テーブルの情報を基に HDD 内検索
520
視聴コンテンツ選択
540
メタデータ復号（鍵：Ki）
522
契約条件を確認、記入し 視聴選択
541
契約条件より課金処理
524
契約条件よりメタデータの 契約情報作成
525
メタデータをメタデータ1,2に 分離
526
Ki'生成
527
メタデータ２を暗号化（鍵:Ki'）
528
HDD に蓄積
542
メタデータ１（Ki'）を 暗号化（鍵：Km2）
530
CA モジュールに蓄積
531
コンテンツ復号（鍵：Kk）
543

【図２０】


A
101
3
A
CAモジュール
600
A
CAモジュール
604
A
PDR
リムーバブルメディア
PDR
リムーバブルメディア
CAモジュールAによる
個人登録処理
5
CAモジュールAによる
個人認証

【図２５】



フロントページの続き

(51) Int.Cl.[7]	識別記号	FI		テーマコード(参考)
H04N	7/16	H04N	5/91	L
				P
	7/167		7/167	Z

(72)発明者　山崎　伊織
東京都千代田区神田駿河台四丁目６番地
株式会社日立製作所放送・通信システム推進事業部内

Fターム(参考)　5C025 BA25 BA27 BA28 BA30 DA01 DA04 DA10
5C053 FA20 FA23 FA24 GA20 LA07 LA14
5C064 BA07 BB01 BB02 BC10 BC17 BC20 BD08 BD09 CA14 CB01 CC04 CC06
5J104 AA16 AA34 DA04 EA04 EA17 JA03 NA02 PA14